CA ARCserve® Central Protection Manager

Guida per l'utente

r16

Riferimenti ai prodotti CA Technologies

Questo documento è valido per i seguenti prodotti di CA Technologies:

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication e High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

Contattare il servizio di Supporto tecnico

Per l'assistenza tecnica in linea e un elenco completo delle sedi, degli orari del servizio di assistenza e dei numeri di telefono, contattare il Supporto tecnico visitando il sito Web all'indirizzo http://www.ca.com/worldwide.

Collegamenti di supporto per CA ARCserve Central Applications:

CA Support Online offre un insieme di risorse per la risoluzione di problemi tecnici e fornisce l'accesso a informazioni di prodotto importanti. Il CA Support consente di accedere facilmente a fonti di supporto disponibili in qualunque momento. I seguenti collegamenti consentono l'accesso a vari siti di CA Support disponibili per l'utente:

- **Informazioni sul Supporto tecnico** - Questo collegamento fornisce informazioni sui programmi di manutenzione e le offerte di supporto, inclusi termini e condizioni, richieste, obiettivi del livello di servizio e ore di servizio.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Registrazione al Supporto tecnico** - Questo collegamento consente di accedere al modulo di registrazione in linea di CA Support, utile per l'attivazione del supporto per il prodotto.

  https://support.ca.com/prodinfo/supportregistration

- **Accesso al Supporto tecnico** - Questo collegamento consente di accedere alla pagina del supporto One-Stop di CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Modifiche apportate alla documentazione

La presente documentazione contiene commenti e suggerimenti degli utenti, correzioni e altre modifiche minori per migliorare le modalità di utilizzo e il funzionamento del prodotto o la documentazione stessa.

Di seguito sono riportati gli aggiornamenti apportati alla documentazione dalla versione di disponibilità generale:

Aggiornamento 7

- Aggiunta della sezione Opzioni del processo di unione (a pagina 72). Questo argomento contiene due opzioni nuove: Sospendi processo di unione (a pagina 72) e Riprendi processo di unione (a pagina 73) della schermata Nodo. Questi argomenti descrivono la modalità di interruzione o ripresa di un processo di unione per un nodo specifico.
- Aggiornamento della sezione Definizione delle impostazioni di protezione (a pagina 89). Questo argomento contiene informazioni sulle opzioni di impostazione della memorizzazione. I criteri di memorizzazione consentono di specificare il numero di punti di ripristino o di set di ripristino che si desidera memorizzare.
- Aggiornamento della sezione Definizione degli avvisi di posta elettronica (a pagina 128). La presente sezione contiene aggiornamenti circa gli avvisi di backup per i processi di unione. È ora possibile ricevere un avviso per i processi di unione interrotti, ignorati, non riusciti o arrestati in modo anomalo. Inoltre, è stata aggiunta una nuova opzione per l'invio di avvisi relativi a processi di unione eseguiti correttamente.

Aggiornamento 6

- Aggiornamento della sezione Configurazione delle pianificazioni di rilevamento (a pagina 38). La sezione include un elenco Active Directory per l'impostazione di una pianificazione per il rilevamento dei nodi.
- Aggiornamento della sezione Configurazione delle impostazioni dei messaggi di posta elettronica e di avviso (a pagina 38). Per poter includere gli avvisi relativi ai nodi rilevati, il titolo e i contenuti della presente sezione sono stati aggiornati.
- Aggiornamento della sezione Aggiornamento dei nodi (a pagina 68). La sezione descrive la modalità di aggiornamento di nodi multipli contemporaneamente mediante le credenziali esistenti o la specificazione di nuove credenziali. È possibile imporre al server la gestione dei nodi selezionati.
- Aggiornamento della sezione Aggiunta di gruppi di nodi (a pagina 78). La presente sezione sostituisce il gruppo nodi Non assegnato con Nodi senza un criterio, nonché il gruppo nodi Nessun raggruppamento con Nodi senza un gruppo.

- Aggiornamento della sezione Distribuzione dei nodi su CA ARCserve D2D (a pagina 84). La sezione è stata aggiornata per includere la versione più recente di CA ARCserve D2D per la distribuzione su un nodo e supportare le versioni precedente di CA ARCserve D2D. È stato inoltre incluso un nuovo pulsante denominato Seleziona/Deseleziona tutto per la selezione dei nodi.
- Aggiornamento della sezione Definizione delle destinazioni di copia file (a pagina 114). La sezione è stata aggiornata per includere Fujitsu Cloud (Windows Azure) come tipo di fornitore per la configurazione cloud.
- La presente versione di aggiornamento consente di visualizzare lo stato di una distribuzione di criteri nella colonna Criterio.

Aggiornamento 5

- Informazioni sulla schermata di gestione dei nodi (a pagina 59). Rimozione della cattura di schermata relativa alla visualizzazione del nodo per modifiche dell'interfaccia utente.
- Aggiunta di gruppi di nodi (a pagina 78). Questo argomento è stato aggiornato per includere i filtri Gruppo e Nome nodo.
- Distribuzione di CA ARCserve D2D sui nodi (a pagina 84). Questo argomento è stato aggiornato per includere il filtro Gruppo e Nome nodo nella schermata Distribuzione D2D.
- Assegnazione e annullamento dell'assegnazione di nodi dai criteri (a pagina 140). Questo argomento è stato aggiornato per includere i filtri Gruppo e Nome nodo nella schermata Assegna/Annulla assegnazione criterio.

Aggiornamento 4

- Aggiunta della sezione Disinstallazione di CA ARCserve Central Protection Manager (a pagina 23). Questo scenario descrive le modalità disponibili per la disinstallazione dell'applicazione.
- Aggiunta della sezione Utilizzo di CA ARCserve Central Protection Manager per il backup dei nodi CA ARCserve D2D (a pagina 52). Questo scenario descrive la procedura per la creazione di un criterio di backup di base per eseguire il backup dei nodi CA ARCserve D2D.
- Aggiunta della sezione Esecuzione di un backup immediato (a pagina 141). Questo argomento descrive la modalità di esecuzione di un processo di backup ad hoc.
- Aggiunta della sezione Visualizzazione delle informazioni sullo stato del processo (a pagina 144). Questo argomento descrive le modalità di visualizzazione in tempo reale delle informazioni sui processi di backup in corso.
- Aggiornamento di tutti gli argomenti relativi al ripristino dei dati (a pagina 145). È ora possibile inoltrare i processi di ripristino direttamente dalla schermata Nodo.
- Aggiunta della sezione Modifica del protocollo di comunicazione del server (a pagina 167). Questo argomento descrive la procedura per la modifica del protocollo di comunicazione utilizzato dai componenti di CA ARCserve Central Applications da HTTP a HTTPS e da HTTPS a HTTP mediante un file batch.

Aggiornamento 1

- Aggiunta della sezione Integrazione di CA ARCserve Central Protection Manager con gli strumenti del server di gestione IT (a pagina 169). Questa sezione descrive le modalità di integrazione di CA ARCserve Central Protection Manager con gli strumenti di gestione dell'infrastruttura del server di gestione IT, ad esempio, Nimsoft e Kaseya.

Sommario

Capitolo 1: Introduzione a CA ARCserve Central Protection Manager 11

Capitolo 2: Installazione di CA ARCserve Central Protection Manager 15

Capitolo 3: Introduzione a CA ARCserve Central Protection Manager 35

Capitolo 4: Utilizzo di CA ARCserve Central Protection Manager 51

Capitolo 5: Integrazione di CA ARCserve Central Protection Manager con gli strumenti del server di gestione IT 169

Capitolo 6: Risoluzione dei problemi relativi a CA ARCserve Central Protection Manager 185

Indice 211

Capitolo 1: Introduzione a CA ARCserve Central Protection Manager

Questa sezione contiene i seguenti argomenti:

Introduzione

CA ARCserve Central Applications combina la protezione dei dati principali e le tecnologie di gestione con un ecosistema mirato di applicazioni che funzionano all'unisono al fine di facilitare la protezione, la copia, lo spostamento e la trasformazione dei dati on-premise e off-premise all'interno di ambienti globali.

Le applicazioni CA ARCserve Central Applications possono essere utilizzate, gestite e installate facilmente. Questa soluzione consente alle organizzazioni un controllo automatizzato delle informazioni al fine di prendere decisioni consapevoli sull'accesso, sulla disponibilità e sulla protezione dei dati in base al valore di business complessivo.

Una delle applicazioni offerte da CA ARCserve Central Applications è l'applicazione CA ARCserve Central Protection Manager. CA ARCserve Central Protection Manager consente di gestire gli ambienti CA ARCserve D2D e CA ARCserve Backup da una posizione centrale. Singole applicazioni permettono un livello limitato di gestione dei nodi mentre con l'applicazione CA ARCserve Central Protection Manager è possibile:

- Aggiungere uno o più nodi
- Rilevare i nodi dal server di Active Directory
- Rilevare e aggiungere i computer virtuali gestiti da un hypervisor
- Rilevare l'applicazione sui server aggiunti
- Creare e assegnare criteri di CA ARCserve D2D
- Inoltrare i processi di ripristino per i server CA ARCserve D2D gestiti
- Sincronizzare i dati dai server CA ARCserve Backup e CA ARCserve D2D gestiti
- Eseguire la distribuzione di CA ARCserve D2D

Modalità di funzionamento dell'applicazione

CA ARCserve Central Protection Manager consente di visualizzare e gestire i nodi protetti da una posizione centrale.

Avviare CA ARCserve Central Protection Manager facendo clic su Start > Tutti i programmi > CA > Central Applications > CA ARCserve Central Protection Manager. Verrà visualizzata la pagina principale di CA ARCserve Central Protection Manager, dalla quale sarà possibile accedere a qualsiasi funzione di CA ARCserve Central Protection Manager mediante le seguenti funzionalità di navigazione:

- **Nodo** - Consente di utilizzare diversi strumenti per gestire i nodi e i gruppi di nodi, rilevare i nodi, effettuare la distribuzione di CA ARCserve D2D sui nodi e sincronizzare i dati.
- **Criteri** - Consente di aggiungere, modificare, eliminare, copiare e assegnare criteri CA ARCserve D2D. Questa funzionalità visualizza i dettagli del criterio e consente di assegnare o annullare l'assegnazione di un nodo dal criterio CA ARCserve D2D corrispondente.
- **Configurazione** - Consente di configurare le impostazioni del database, la sincronizzazione dei dati di CA ARCserve Backup, l'esplorazione delle risorse di archiviazione (SRM), il rilevamento automatico, la posta elettronica, gli aggiornamenti, le preferenze, l'account di amministratore, la distribuzione di D2D e il server di gestione IT.
- **Visualizza registri** - Consente di visualizzare i registri attività per ciascun nodo CA ARCserve Central Protection Manager visualizza tutti i messaggi di registro associati al nodo. È possibile filtrare l'elenco in base alla gravità dei messaggi visualizzati (Tutto, Informazioni, Errori, Avvisi, o Errori e avvisi), al tipo di modulo (Tutto, Comune, Importa nodi dal rilevamento, Importa nodi da hypervisor, Importa nodi da file, Gestione criterio, Sincronizzazione di CA ARCserve Backup, Sincronizzazione di CA ARCserve D2D, Aggiornamenti per CA ARCserve D2D, Aggiornamenti e Invia i processi di backup CA ARCserve D2D) oppure al nome del nodo.

Bookshelf di CA ARCserve Central Applications

Gli argomenti contenuti nella Guida in linea di CA ARCserve Central Applications sono disponibili anche nella Guida per l'utente in formato PDF. La versione PDF più recente di questa guida e la Guida in linea sono accessibili dal Bookshelf di CA ARCserve Central Applications.

Nei file Note di rilascio di CA ARCserve Central Applications sono contenute informazioni relative ai requisiti di sistema, al supporto di sistemi operativi, al supporto per il recupero delle applicazioni e altre informazioni che può essere necessario conoscere prima di installare il prodotto. I file di Note di rilascio contengono inoltre un elenco di problemi noti di cui l'utente deve essere a conoscenza prima di utilizzare CA ARCserve Central Applications. La versione più recente delle note di rilascio è disponibile nel Bookshelf di CA ARCserve Central Applications.

Capitolo 2: Installazione di CA ARCserve Central Protection Manager

Questa sezione contiene i seguenti argomenti:

Attività preliminari all'installazione

Prima di installare l'applicazione, completare le seguenti attività preliminari:

- Consultare il file delle Note di rilascio. Le Note di rilascio descrivono i requisiti di sistema, informazioni sui sistemi operativi supportati e un elenco di problemi noti per questa versione di CA ARCserve Central Protection Manager.
- Verificare che i sistemi soddisfino i requisiti hardware e software minimi necessari per l'installazione dell'applicazione.
- Verificare che l'account Windows disponga dei privilegi di amministratore o equivalenti per l'installazione del software sui computer in cui si desidera installare CA ARCserve Central Protection Manager.
- Verificare di disporre dei nomi utente e delle password dei computer su cui si sta procedendo all'installazione dell'applicazione di cui si è in possesso.

- Verificare che il server in cui è installato CA ARCserve Central Protection Manager e i nodi in cui si desidera distribuire i criteri possano comunicare tra loro utilizzando i rispettivi nomi host. Per verificare che i server e i nodi CA ARCserve Central Protection Manager siano in grado di comunicare tra loro, procedere come segue:
  - Dal server CA ARCserve Central Protection Manager, eseguire il ping dei nodi utilizzando i nomi host dei nodi.
  - Dai nodi che si desidera proteggere, eseguire il ping di CA ARCserve Central Protection Manager utilizzando il nome host del server.
- CA ARCserve Central Protection Manager consente l'installazione di CA ARCserve D2D r16 e l'aggiornamento di CA ARCserve D2D r15 a CA ARCserve D2D r16 su nodi remoti mediante l'utilità Distribuzione. Per eseguire il backup dei dati su nodi remoti mediante CA ARCserve D2D r16, è necessario ottenere le licenze di CA ARCserve D2D r16 e applicarle ai nodi. Se le licenze non vengono applicate entro 31 giorni dalla data di installazione o aggiornamento di CA ARCserve D2D r16 sui nodi, il funzionamento di CA ARCserve D2D verrà interrotto.
- I supporti di installazione di CA ARCserve Central Protection Manager dispongono di Microsoft SQL Server 2008 R2 Express Edition, che corrisponde all'applicazione di database minima richiesta per il supporto del database CA ARCserve Central Protection Manager. Se si desidera utilizzare Microsoft SQL Server per il supporto del database CA ARCserve Central Protection Manager, installare Microsoft SQL Server sul server o su un server remoto CA ARCserve Central Protection Manager prima di installare CA ARCserve Central Protection Manager. Se la routine di installazione rileva una versione di Microsoft SQL Server non supportata, non sarà possibile completare l'installazione. Per ulteriori informazioni sulle versioni supportate di Microsoft SQL Server, consultare le Note di rilascio.

Considerazioni sull'installazione

Prima di installare CA ARCserve Central Virtual Standby, tenere presenti le seguenti considerazioni sull'installazione:

- Il pacchetto di installazione di CA ARCserve Central Applications installa un modulo denominato CA ARCserve Central Applications Server. CA ARCserve Central Applications Server è un modulo comune a tutte le applicazioni CA ARCserve Central Applications. Il modulo contiene il servizio Web, i file binari e le configurazioni che consentono alle applicazioni CA ARCserve Central Applications di comunicare tra loro.

  Quando si installa CA ARCserve Central Applications, il modulo CA ARCserve Central Applications Server viene installato prima dei componenti del prodotto. Nel caso in cui sia necessario applicare una patch a CA ARCserve Central Applications, la patch aggiorna il modulo prima di aggiornare i componenti del prodotto.

- Quando CA ARCserve D2D viene distribuito sui nodi remoti, VMware Virtual Disk Development Kit (VDDK) 1.2.1 viene installato da CA ARCserve Central Protection Manager sui nodi di destinazione. I supporti di installazione di CA ARCserve Central Protection Manager includono file richiesti per l'installazione di VMware Virtual Disk Development Kit (VDDK) 1.2.1 sul server CA ARCserve Central Protection Manager e il nodo di destinazione. Non è pertanto necessario scaricare i file di installazione di VDDK dal sito Web di VMware per poter eseguire la distribuzione di CA ARCserve D2D ai nodi remoti.

Installazione di CA ARCserve Central Protection Manager

La procedura guidata di installazione consente all'utente di installare una o più applicazioni di CA ARCserve Central Applications.

Nota: prima di installare l'applicazione, consultare il file delle Note di rilascio e verificare che tutte le attività descritte nella sezioneAttività preliminari siano complete.

Per installare CA ARCserve Central Protection Manager

1. Scaricare il pacchetto di installazione di CA ARCserve Central Applications sul computer su cui si desidera installare l'applicazione, quindi fare doppio clic sul file di installazione.

   I contenuti del pacchetto di installazione verranno estratti sul computer e verrà visualizzata la finestra di dialogo Componenti richiesti.

2. Fare clic su Installa.

   Nota: la finestra di dialogo Componenti richiesti viene visualizzata solo se il programma di installazione non rileva che i componenti richiesti sono installati sul computer di destinazione.

   Al termine dell'installazione dei componenti richiesti, verrà visualizzata la finestra di dialogo Contratto di licenza.

3. Selezionare le opzioni necessarie, quindi fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Configurazione.

4. Sulla finestra di dialogo Configurazione, completare i seguenti campi:

   - **Componenti** - Specificare le applicazioni che si desidera installare.

     Nota: se l'applicazione viene installata mediante il pacchetto di installazione, è possibile installare più applicazioni simultaneamente.

   - **Posizione** - Accettare la posizione di installazione predefinita o fare clic su Sfogliare per specificare una posizione di installazione alternativa. La directory predefinita è la seguente:

     ```
     C:\Programmi\CA\ARCserve Central Applications
     ```

   - **Informazioni sul disco** - Verificare che il disco rigido disponga dello spazio sufficiente per l'installazione delle applicazioni.

   - **Nome dell'amministratore di Windows** - Specificare il nome utente dell'account di amministratore di Windows utilizzando la seguente sintassi:

     ```
     Dominio\Nome utente
     ```

   - **Password** - Specificare la password per l'account utente.

   - **Specificare il numero di porta** - Specificare il numero di porta da utilizzare per la comunicazione con l'interfaccia utente Web. Si consiglia di accettare il numero di porta predefinito. Il numero predefinito della porta è il seguente:

     ```
     8015
     ```

     Nota: per specificare un numero di porta alternativo, sarà necessario indicare un numero di porta compreso fra 1024 e 65535. Prima di indicare un numero di porta alternativo, verificare che il numero specificato sia libero e disponibile per l'uso. Il programma di installazione, infatti, non consente di installare l'applicazione se la porta selezionata non è disponibile per l'uso.

   - **Usa https per la comunicazione Web -** Specificare l'utilizzo della comunicazione HTTPS per la trasmissione dati. Per impostazione predefinita questa opzione è deselezionata.

     Nota: il protocollo HTTPS (protetto) fornisce un livello di protezione superiore rispetto alla comunicazione HTTP. Il protocollo di comunicazione HTTPS è consigliato se si trasmettono informazioni riservate sulla rete.

- **Consenti al programma di installazione di registrare servizi/programmi di CA ARCserve Central Applications su Windows Firewall come eccezioni** - Verificare che la casella di controllo accanto a questa opzione sia selezionata. Le eccezioni firewall sono necessarie se si desidera configurare e gestire CA ARCserve Central Applications da computer remoti.

  Nota: per gli utenti locali, non è necessario registrare le eccezioni firewall.

Fare clic su Avanti.

Verrà visualizzata la finestra di dialogo Impostazioni database.

5. Nella finestra di dialogo delle impostazioni del database, fare clic sull'elenco a discesa al lato del campo Scegliere un tipo di database, quindi specificare una delle seguenti opzioni:

   - Database predefinito ARCserve Central Applications
   - Microsoft SQL Server

   Dopo aver selezionato un tipo di database, nella finestra di dialogo delle impostazioni del database verranno visualizzate le opzioni relative al database specificato.

6. Eseguire una delle seguenti operazioni:

   - **Database predefinito di ARCserve Central Protection Applications** - Completare i seguenti campi della finestra di dialogo delle impostazioni del database:

     - **Specificare il percorso di installazione** - Specificare la posizione in cui si desidera installare il database predefinito di CA ARCserve Central Applications. È possibile accettare il percorso predefinito o specificare un percorso alternativo.
     - **Specificare il percorso del file di dati** - Specificare la posizione in cui si desidera installare i file di dati per il database predefinito di CA ARCserve Central Applications. È possibile accettare il percorso predefinito o specificare un percorso alternativo.

     Nota: il database predefinito di CA ARCserve Central Applications non supporta la comunicazione remota. Pertanto, è necessario installare il database predefinito e il file di dati sul computer in cui si sta installando l'applicazione.

- **Database Microsoft SQL Server** - Completare i seguenti campi della finestra di dialogo delle impostazioni del database:
  - **Tipo di server SQL** - Specificare il tipo di comunicazione che l'applicazione dovrà utilizzare per comunicare con il database di SQL Server.

    Locale - Specificare Locale quando l'applicazione e il server SQL sono installati sullo stesso computer.

    Remoto - Specificare Remoto quando l'applicazione e il server SQL sono installati su computer differenti.
  - **Nome Server SQL** - Se il tipo di server SQL specificato è Remoto, specificare il nome del server SQL remoto. Se il server SQL viene utilizzato in locale, selezionare il server dall'elenco a discesa.
  - **Protezione** - Specificare il tipo di credenziali che si desidera utilizzare per l'autenticazione su SQL Server.

    Usa protezione Windows - Specificare questa opzione per effettuare l'autenticazione utilizzando le credenziali di Windows.

    Usa protezione SQL Server - Specificare questa opzione per effettuare l'autenticazione utilizzando le credenziali di SQL Server. Specificare, quindi, l'ID di accesso e la password per l'account di SQL Server.
  - **Sovrascrivi il database esistente** - Specificare questa opzione se si desidera consentire al programma di installazione di rilevare e sovrascrivere il database CA ARCserve Central Applications esistente.

Fare clic su Installa.

Al completamento dell'installazione, verrà visualizzata la finestra di dialogo Rapporto installazione.

7. La finestra di dialogo Rapporto installazione presenta un riepilogo di installazione. Per verificare la presenza di aggiornamenti per l'applicazione, fare clic su Verifica aggiornamenti e fare clic su Fine.

L'applicazione verrà installata.

Installare CA ARCserve Central Protection Manager in modalità invisibile all'utente

CA ARCserve Central Applications consente di installare
CA ARCserve Central Protection Manager in modalità invisibile all'utente. Se si utilizza l'installazione invisibile all'utente, non sarà necessaria alcuna operazione da parte dell'utente. Di seguito è descritta la procedura per installare l'applicazione in modalità invisibile utilizzando la riga di comando di Windows.

Per installare CA ARCserve Central Protection Manager in modalità invisibile all'utente

1. Aprire la riga di comando di Windows nel computer in cui si desidera iniziare il processo di installazione invisibile all'utente.

2. Scaricare il pacchetto di installazione autoestraente di
   CA ARCserve Central Applications.

   Avviare il processo di installazione invisibile all'utente utilizzando la seguente sintassi della riga di comando:

   ```
   "CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<INSTALLDIR> -
   Port:<PORT> -U:<UserName> -P:<Password> -Products:<ProductList>"
   ```

   Uso:

   s

   Consente di avviare il pacchetto di file eseguibile in modalità invisibile all'utente.

   v

   Consente di specificare ulteriori opzioni della riga di comando.

   q

   Consente di installare l'applicazione in modalità invisibile all'utente.

   -Percorso:<INSTALLDIR>

   (Facoltativo) Consente di specificare il percorso di destinazione dell'installazione.

   Esempio:

   ```
   -Percorso:C:\Programmi\CA\ARCserve Central Applications
   ```

   Nota: se il valore di INSTALLDIR contiene uno spazio, racchiudere il percorso tra virgolette e barre rovesciate. Inoltre, il percorso non può terminare con una barra rovesciata.

-Port:<PORTA>

(Facoltativo) Consente di specificare il numero di porta per la comunicazione.

Esempio:

```
-Port:8015
```

-U:<NomeUtente>

Consente di specificare il nome utente da utilizzare per installare ed eseguire l'applicazione.

Nota: il nome utente deve corrispondere a un account amministrativo o a un account con privilegi amministrativi.

-P:<Password>

Consente di specificare la password per il nome utente.

-Products:<Elenco prodotti>

(Facoltativo) Consente di specificare l'installazione in modalità invisibile all'utente di CA ARCserve Central Applications. Se non si specifica un valore per questo argomento, durante la procedura di installazione invisibile all'utente vengono installati tutti i componenti di CA ARCserve Central Applications.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

Tutte le applicazioni CA ARCserve Central Applications

TUTTO

Nota: gli esempi riportati di seguito descrivono la sintassi per eseguire l'installazione di una o più applicazioni CA ARCserve Central Applications in modalità invisibile all'utente:

```
-Products:CMX64
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:ALL
```

L'applicazione verrà installata in modalità invisibile all'utente.

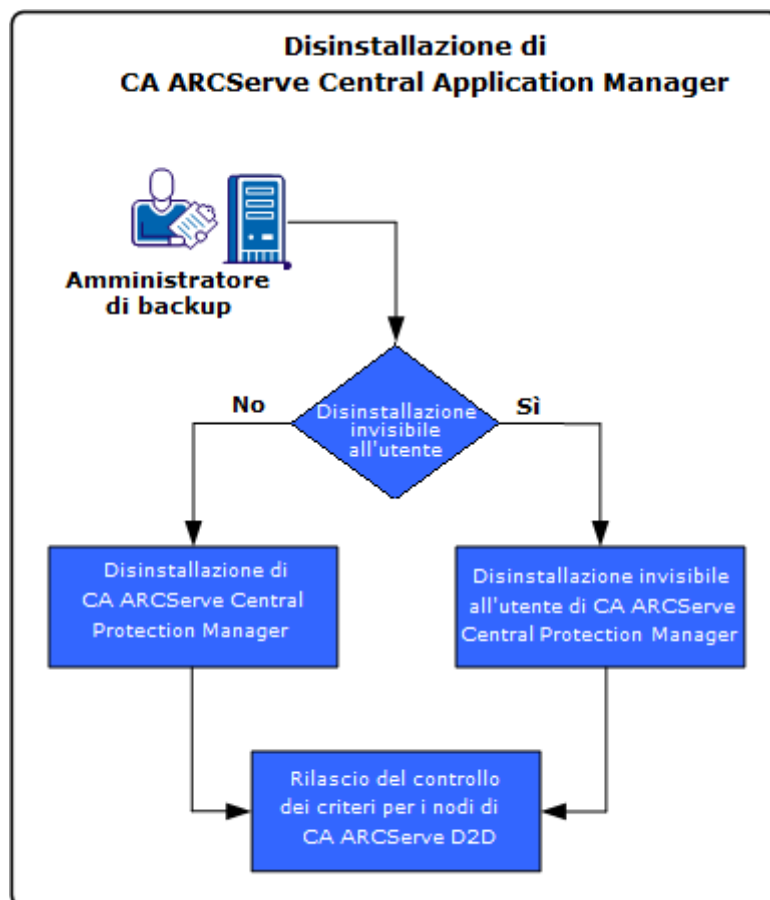
Disinstallazione di CA ARCserve Central Protection Manager

Per eseguire la disinstallazione CA ARCserve Backup utilizzare uno dei seguenti metodi:

- Disinstallazione standard - Questo metodo consente di disinstallare l'applicazione dal Pannello di controllo di Windows.
- Disinstallazione invisibile all'utente - Questo metodo consente di eseguire disinstallazioni non previste mediante la riga di comando di Windows.

Annullamento dell'assegnazione dei criteri

Come procedura ottimale, si raccomanda di annullare l'assegnazione di tutti i criteri dai nodi a cui sono assegnati prima di procedere alla disinstallazione dell'applicazione. Si consiglia questo tipo di approccio in quanto non è possibile specificare le impostazioni di backup di CA ARCserve D2D sul nodo se il criterio di CA ARCserve Central Protection Manager è assegnato al nodo. Inoltre, non è possibile annullare l'assegnazione dei criteri dai nodi una volta disinstallata l'applicazione. CA ARCserve D2D include un'utilità di riga di comando che consente di annullare l'assegnazione dei criteri dai nodi in seguito alla disinstallazione dell'applicazione.

Il diagramma seguente mostra la procedura di disinstallazione dell'applicazione:

Attività	Argomento
Disinstallazione standard mediante il Pannello di controllo di Windows.	Disinstallazione di CA ARCserve Central Protection Manager. (a pagina 25)
Disinstallazione invisibile all'utente mediante la riga di comando di Windows.	Disinstallazione di CA ARCserve Central Protection Manager in modalità invisibile all'utente. (a pagina 26)
Annullamento dell'assegnazione dei criteri sui nodi in seguito alla disinstallazione di CA ARCserve Central Protection Manager.	Rilascio del controllo di criteri per i nodi di CA ARCserve D2D (a pagina 27).

Disinstallazione di CA ARCserve Central Protection Manager

La disinstallazione di CA ARCserve Central Protection Manager può essere effettuata anche mediante l'opzione Programmi e funzionalità del Pannello di controllo di Windows.

Procedere come descritto di seguito:

1. Accedere al computer da cui si desidera disinstallare l'applicazione.

   Nota: è necessario accedere con un account amministrativo o un account con privilegi amministrativi.

2. Dal menu Start di Windows, fare clic su Start e selezionare Pannello di controllo per aprire il pannello di controllo di Windows.
3. Fare clic su Programmi e funzionalità per visualizzare la finestra Disinstalla o modifica programma.
4. Individuare e fare clic su CA ARCserve Central Protection Manager.

   Fare clic con il pulsante destro del mouse sull'applicazione, quindi fare clic su Disinstalla dal menu di scelta rapida.

   Seguire le istruzioni visualizzate sullo schermo per completare la disinstallazione.

L'applicazione verrà disinstallata.

Disinstallazione di CA ARCserve Central Protection Manager in modalità invisibile all'utente

CA ARCserve Central Applications consente di disinstallare CA ARCserve Central Protection Manager in modalità invisibile all'utente. Se si utilizza l'installazione invisibile all'utente, non sarà necessaria alcuna operazione da parte dell'utente. Di seguito si descrive la procedura per installare l'applicazione in modalità invisibile all'utente utilizzando la riga di comando di Windows.

Procedere come descritto di seguito:

1. Accedere al computer da cui si desidera disinstallare l'applicazione.

   Nota: è necessario accedere con un account amministrativo o un account con privilegi amministrativi.

2. Aprire la riga di comando di Windows ed eseguire il seguente comando per avviare il processo di disinstallazione invisibile all'utente:

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ProductCode>
   ```

   Oppure

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ALL>
   ```

   Esempio: la sintassi seguente consente di disinstallare l'applicazione in modalità invisibile all'utente.

   ```
   "%Programmi%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED05FE-D895-4FD5-B964-001928BD2D62}
   ```

   Uso:

   <INSTALLDIR>

   Consente di specificare la directory in cui è installata l'applicazione.

   Nota: eseguire la sintassi corrispondente all'architettura del sistema operativo del computer.

   <CodiceProdotto>

   Consente di specificare l'applicazione da disinstallare in modalità invisibile all'utente. Utilizzare i seguenti codici di prodotto per installare CA ARCserve Central Applications in modalità invisibile all'utente:

   CA ARCserve Central Protection Manager

   {CAED05FE-D895-4FD5-B964-001928BD2D62}

   CA ARCserve Central Host-Based VM Backup

   {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

   CA ARCserve Central Reporting

   {CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

   CA ARCserve Central Virtual Standby

```
{CAED4835-964B-484B-A395-E2DF12E6F73D}
```

L'applicazione verrà disinstallata in modalità invisibile all'utente.

Rilascio del controllo di criteri per i nodi di CA ARCserve D2D

Il processo di disinstallazione di CA ARCserve Central Protection Manager non annulla l'assegnazione dei criteri di backup dai nodi CA ARCserve D2D. Questo comportamento non consente di specificare le impostazioni di backup direttamente sui nodi CA ARCserve D2D in seguito alla disinstallazione di Protection Manager. Come procedura ottimale, prima di procedere alla disinstallazione dell'applicazione, annullare l'assegnazione di tutti i criteri dai nodi a cui sono assegnati. Se questa operazione non viene eseguita, è possibile rilasciare il controllo dei criteri per i nodi mediante un'utilità progettata specificatamente per questo scopo.

Procedere come descritto di seguito:

1. Accedere al nodo di CA ARCserve D2D.
2. Aprire la riga di comando di Windows e accedere alla seguente directory:

   ```
   C:\Program Files\CA\ARCserve D2D\BIN
   ```

3. Eseguire ARCCentralAppMgrUtility.exe utilizzando la sintassi seguente:

```
ARCCentralAppMgrUtility.exe -clean pm|hbvb|vs [-debug]
```

pm|hbvb|vs

Definisce l'applicazione che si desidera rilasciare dal controllo del nodo di CA ARCserve D2D. Specificare uno dei seguenti argomenti:

pm

CA ARCserve Central Protection Manager

hbvb

CA ARCserve Central Host-Based VM Backup

vs

CA ARCserve Central Virtual Standby

-debug

L'opzione -debug non è obbligatoria. Specificare questa opzione se si desidera generare un file di registro di debug archiviato nella directory seguente:

```
<D2D_Home>\Log\ARCCentralAppMgrUtility.log
```

Esempio: l'esempio riportato di seguito descrive la sintassi per il rilascio del controllo dei criteri dal nodo.

```
ARCCentralAppMgrUtility.exe -clean pm
```

Il controllo dei criteri viene rilasciato per il nodo.

Relazione tra il processo di installazione e i sistemi operativi

Il processo di installazione di CA ARCserve Central Applications aggiorna i vari componenti del sistema operativo Windows utilizzando un modulo di installazione denominato MSI (Microsoft Installer Package). I componenti inclusi nel file MSI consentono a CA ARCserve Central Applications di eseguire operazioni personalizzate che permettono di installare, aggiornare o disinstallare CA ARCserve Central Applications.

Nella tabella seguente vengono descritte le azioni personalizzate e i componenti interessati.

Nota: tutti i pacchetti MSI di CA ARCserve Central Applications richiamano i componenti elencati in questa tabella quando si installa e disinstalla CA ARCserve Central Applications.

Componente	Descrizione
CallAllowInstall	Consente al processo di installazione di controllare le condizioni relative all'installazione corrente di CA ARCserve Central Applications.
CallPreInstall	Consente al processo di installazione di leggere e scrivere le proprietà del pacchetto MSI. Ad esempio, consente di leggere il percorso di installazione di CA ARCserve Central Applications dal pacchetto MSI.
CallPostInstall	Consente al processo di installazione di eseguire varie operazioni relative all'installazione. Ad esempio, la registrazione di CA ARCserve Central Applications nel Registro di sistema di Windows.
CallAllowUninstall	Consente al processo di disinstallazione di controllare le condizioni relative all'installazione corrente di CA ARCserve Central Applications.
CallPreUninstall	Consente al processo di disinstallazione di eseguire varie operazioni relative alla disinstallazione. Ad esempio, l'annullamento della registrazione di CA ARCserve Central Applications dal Registro di sistema di Windows.
CallPostUninstall	Consente al processo di disinstallazione di eseguire varie attività dopo la disinstallazione dei file installati. Ad esempio, consente di rimuovere i file restanti.

Componente	Descrizione
ShowMsiLog	Consente di visualizzare il file di registro di Windows Installer in Notepad se si seleziona la casella di controllo Mostra registro di Windows Installer nelle finestre di dialogo di completamento dell'installazione, di errore dell'installazione o di interruzione dell'installazione. Sarà quindi necessario fare clic su Fine. (funziona solo con Windows Installer 4.0.)
ISPrint	Stampa il contenuto di un controllo ScrollableText in una finestra di dialogo. Azione personalizzata del file .dll di Windows Installer. Il nome del file DLL è SetAllUsers.dll e il punto di ingresso è PrintScrollableText.
CheckForProductUpdates	Utilizza FLEXnet Connect per verificare la disponibilità di aggiornamenti di prodotto. Questa azione personalizzata avvia un file eseguibile denominato Agent.exe e trasmette la seguente istruzione: /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Utilizza FLEXnet Connect per verificare la disponibilità di aggiornamenti di prodotto al riavvio. Questa azione personalizzata avvia un file eseguibile denominato Agent.exe e trasmette la seguente istruzione: /au[ProductCode] /EndOfInstall /Reboot

- **Directory aggiornate** - Per impostazione predefinita, il processo di installazione installa e aggiorna i file di CA ARCserve Central Applications nelle seguenti directory:

  `C:\Programmi\CA\ARCserve Central Applications`

  È possibile installare CA ARCserve Central Applications nella directory di installazione predefinita oppure in una directory alternativa. Il processo di installazione copia vari file di sistema nella directory seguente:

  `C:\WINDOWS\SYSTEM32`

- **Aggiornamento delle chiavi del Registro di sistema di Windows** - Durante il processo di installazione vengono aggiornate le seguenti chiavi del Registro di sistema di windows:

  Chiavi predefinite del Registro di sistema:

  `HKLM\SOFTWARE\CA\CA ARCserve Central Applications`

  Il processo di installazione modifica e crea nuove chiavi del Registro di sistema, in base alla configurazione del sistema in uso.

- **Applicazioni installate** - Il processo di installazione installa le seguenti applicazioni nel computer in uso:
  - CA Licensing
  - Microsoft Visual C++ 2005 SP1 Redistributable
  - Microsoft Windows Installer 3.1 Redistributable (v2) Package
  - Java Runtime Environment (JRE) 1.6.0_16
  - Tomcat 6.0.32

File binari con informazioni non corrette sulla versione dei file

CA ARCserve Central Applications esegue l'installazione di file binari sviluppati da terze parti, altri prodotti CA, e CA ARCserve Central Applications contenenti informazioni sulla versione dei file incorrette. La seguente tabella descrive tali file binari.

Nome file binario	Origine
UpdateData.exe	CA License
zlib1.dll	Zlib Compression Library

File binari non contenenti il manifesto integrato

CA ARCserve Central Applications installa i file binari sviluppati da terze parti, altri prodotti CA Technologies, e file CA ARCserve Central Applications non contenenti un manifesto integrato o un manifesto di testo. La seguente tabella descrive tali file binari.

Nome file binario	Origine
BaseLicInst.exe	CA License
UpdateData.exe	CA License
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
tomcat6.exe	Tomcat

File binari che richiedono un livello di privilegi di tipo Amministratore nel manifesto

CA ARCserve Central Applications installa file binari sviluppati da terze parti, da altri prodotti CA Technologies e file CA ARCserve Central Applications che richiedono un livello di privilegi di tipo Amministratore o più elevato. Per poter eseguire i servizi, i componenti e le applicazioni di CA ARCserve Central Applications è necessario effettuare l'accesso utilizzando un account amministrativo o un account che dispone di autorizzazioni più elevate. I file binari corrispondenti a tali servizi, componenti e applicazioni includono funzionalità specifiche di CA ARCserve Central Applications non disponibili per un account utente di base. Ne consegue che per completare un'operazione in Windows verrà richiesto di confermare tale operazione mediante l'immissione di una password oppure mediante l'utilizzo di un account che dispone di privilegi di amministrazione.

- **Privilegi di amministratore:** un profilo o un account amministrativo con privilegi di amministratore dispongono di autorizzazioni di lettura, scrittura ed esecuzione per tutte le risorse di sistema e di Windows. Se non si dispone di privilegi di amministratore, verrà richiesto di immettere il nome utente e la password di un utente con tali privilegi per poter continuare.
- **Privilegi più elevati disponibili:** un account con i privilegi più elevati disponibili consiste in un account utente di base e in un account utente avanzato eseguiti con privilegi di amministratore.

La seguente tabella descrive tali file binari.

Nome file binario	Origine
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications

Nome file binario	Origine
RemoteDeploy.exe	CA ARCserve Central Applications
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Capitolo 3: Introduzione a CA ARCserve Central Protection Manager

Le seguenti sezioni descrivono le modalità di configurazione di CA ARCserve Central Protection Manager per la protezione dei nodi CA ARCserve D2D.

Questa sezione contiene i seguenti argomenti:

Verificare che il server CA ARCserve Central Protection Manager sia in grado di comunicare con i nodi

Nota: questo passaggio è facoltativo per la configurazione di CA ARCserve Central Protection Manager per proteggere i nodi.

Per assicurarsi che CA ARCserve Central Protection Manager possa distribuire i criteri ai nodi e proteggere i nodi, verificare che il server Protection Manager e i nodi che si desidera proteggere possano comunicare tra loro utilizzando i rispettivi nomi host.

Per verificare che il server CA ARCserve Central Protection Manager sia in grado di comunicare con i nodi

1. Dal server CA ARCserve Central Protection Manager, eseguire il ping dei nodi da proteggere utilizzando i nomi host dei nodi.
2. Dai nodi che si desidera proteggere, eseguire il ping di CA ARCserve Central Protection Manager utilizzando il nome host del server.

Configurare la pianificazione della sincronizzazione dati di CA ARCserve Backup

La sincronizzazione dati di CA ARCserve Backup consente di configurare il sistema in modo da impostare un orario pianificato e un metodo di ripetizione (numero di giorni, giorno della settimana o giorno del mese) per la sincronizzazione del database CA ARCserve Backup con il database CA ARCserve Central Protection Manager.

Procedere come descritto di seguito:

1. Accedere all'applicazione.
2. Fare clic su Configurazione sulla barra di navigazione per aprire la schermata Configurazione.
3. Nel riquadro Configurazione, fare clic su Pianificazione di sincronizzazione dati di CA ARCserve Backup per visualizzare le opzioni di sincronizzazione dei dati di CA ARCserve Backup.
4. Fare clic su Abilita per abilitare la sincronizzazione dati di CA ARCserve Backup.

   Nota: per impostazione predefinita, la configurazione di sincronizzazione dei dati di CA ARCserve Backup è abilitata.

5. Specificare i parametri seguenti per la pianificazione della sincronizzazione dei dati di CA ARCserve Backup:
   - Metodo di ripetizione
   - Ora pianificata
6. Fare clic su Salva per applicare la pianificazione della sincronizzazione dei dati di CA ARCserve Backup.
7. (Facoltativo) Fare clic su Esegui ora per avviare il processo di sincronizzazione dei dati di CA ARCserve Backup.

Configurazione delle pianificazioni di gestione delle risorse di archiviazione

CA ARCserve Central Protection Manager consente gli amministratori di backup di configurare la pianificazione dei nodi di CA ARCserve D2D per definire l'avvio e la frequenza della raccolta dei dati della gestione delle risorse di archiviazione (SRM). La funzionalità SRM (Gestione delle risorse di archiviazione) raccoglie informazioni su quanto segue:

- Hardware, software e dati di applicazioni per le implementazioni di Microsoft SQL Server e Microsoft Exchange Server.
- Dati sugli indicatori di prestazioni chiave (PKI) da server CA ARCserve D2D gestiti da un server CA ARCserve Central Applications.

  Nota: per i nodi CA ARCserve Backup, CA ARCserve Backup esegue la raccolta dei dati PKI e sincronizza i dati con CA ARCserve Central Protection Manager durante il processo di sincronizzazione dei dati di CA ARCserve Backup.

Procedere come descritto di seguito:

1. Accedere all'applicazione.
2. Selezionare Configurazione dalla barra di navigazione per visualizzare la schermata Configurazione.
3. Nel riquadro Configurazione, fare clic su Configurazione SRM per visualizzare le opzioni di configurazione corrispondenti.
4. Fare clic su Abilita per abilitare la gestione delle risorse di archiviazione (SRM).

   Nota: per impostazione predefinita, la configurazione della gestione delle risorse di archiviazione (SRM) è abilitata.
5. Specificare i parametri seguenti per la pianificazione della gestione delle risorse di archiviazione (SRM):
   - Metodo di ripetizione
   - Ora pianificata

6. Fare clic su Salva per applicare la pianificazione della gestione delle risorse di archiviazione (SRM).
7. (Facoltativo) Fare clic su Esegui ora per avviare il processo di raccolta dei dati SRM.

Configurazione delle pianificazioni di rilevamento

La pianificazione di rilevamento automatico dei nodi può essere impostata su base ricorrente o ad un'ora specificata. Per impostazione predefinita, la configurazione di rilevamento automatico è disabilitata. Per abilitare la configurazione, fare clic sull'opzione Abilita per specificare il tipo di ricorrenza desiderato e l'ora pianificata per l'avvio del rilevamento automatico. È possibile specificare i seguenti parametri di configurazione della pianificazione di rilevamento:

- **Ogni numero di giorni** - Ripete il metodo in base al numero di giorni specificato. (Impostazione predefinita).
- **Ogni giorno della settimana selezionato** - Ripete il metodo nei giorni della settimana specificati. Lunedì, martedì, mercoledì, giovedì e venerdì sono i giorni predefiniti della settimana.
- **Ogni giorno del mese selezionato** - Ripete il metodo nel giorno del mese specificato. Il valore predefinito per il giorno del mese è 1.

Durante la configurazione di una pianificazione per il rilevamento dei nodi, viene visualizzato un elenco Active Directory.

Configurazione delle impostazioni dei messaggi di posta elettronica e di avviso

Le impostazioni di posta elettronica e di avviso possono essere configurate per l'invio automatico degli avvisi nel caso in cui si verifichino le condizioni specificate.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Configurazione per aprire la schermata corrispondente.
2. Dal riquadro Configurazione, fare clic su Configurazione posta elettronica e avvisi per aprire l'opzione Configurazione posta elettronica e avvisi.

3. Completare i seguenti campi:
   - **Servizio** - Specificare il tipo di servizio di posta elettronica dall'elenco a discesa. (Google Mail, Yahoo Mail, Live Mail o Altri).
   - **Server di posta** - Specificare il nome host del server SMTP utilizzato da CA ARCserve Central Applications per l'invio di messaggi di posta elettronica.
   - **Richiede l'autenticazione** - Selezionare questa opzione se il server di posta specificato richiede l'autenticazione. Il Nome account e la Password sono obbligatori.
   - **Oggetto** - Specificare un oggetto di posta elettronica predefinito.
   - **Da** - Specificare l'indirizzo di posta elettronica di invio del messaggio.
   - **Destinatari** - Specificare uno o più indirizzi di posta elettronica, separati da un punto e virgola (;), per l'invio di messaggi di posta elettronica.
   - **Usa SSL** - Selezionare questa opzione se il server di posta specificato richiede la connessione protetta (SSL).
   - **Invia STARTTLS** - Selezionare questa opzione se il server di posta specificato richiede il comando STARTTLS.
   - **Usa formato HTML** - Consente di inviare messaggi di posta elettronica in formato HTML. (selezionato per impostazione predefinita)
   - **Abilita impostazioni proxy** - Selezionare questa opzione se è presente un server proxy, quindi specificare le impostazioni corrispondenti.
4. Fare clic su Messaggio di posta elettronica di verifica per verificare che le impostazioni di configurazione siano corrette.
5. (Facoltativo) Dalla sezione Invia avvisi tramite posta elettronica, fare clic su Nodi rilevati per consentire all'applicazione di inviare messaggi di posta elettronica di avviso al rilevamento di nuovi nodi.
6. Fare clic su Salva.

   Nota: è possibile fare clic su Reimposta per ripristinare i valori salvati precedentemente, oppure fare clic su Elimina per eliminare le impostazioni salvate. L'eliminazione delle impostazioni di posta elettronica e di avviso impediscono la ricezione dei messaggi di posta elettronica di avviso.

La configurazione del server di posta verrà applicata.

Configurazione delle impostazioni del server di gestione IT

CA ARCserve Central Protection Manager consente di inviare messaggi di avviso ai server di gestione IT. Per inviare le informazioni di avviso, configurare il server delle applicazioni per la comunicazione con il server di gestione IT.

Per configurare le impostazioni del server di gestione IT:

1. Accedere a CA ARCserve Central Protection Manager, quindi fare clic su Configurazione della barra di navigazione.
2. Dalla schermata Configurazione, fare clic su Configurazione del server di gestione IT dall'elenco Configurazione.
3. Completare le seguenti opzioni di configurazione del server di gestione IT:
   - Fare clic su Abilita.
   - Fare clic su Nimsoft o Kasaya.
   - Specificare un metodo di ripetizione. Il metodo di ripetizione definisce i giorni della settimana per il rinvio delle notifiche di avviso al server di gestione IT in caso di errore del processo di invio originale. Tale errore può verificarsi nel caso in cui il server di gestione IT non sia in linea o non sia disponibile.
   - Specificare una pianificazione. L'opzione Pianifica definisce l'orario di rinvio delle notifiche di avviso al server Nimsoft.
4. Fare clic su Salva.

La configurazione del server CA ARCserve Central Protection Manager per la comunicazione con il server di gestione IT viene completata.

Nota: è possibile fare clic su Reimposta per tornare ai valori salvati in precedenza.

Configurazione delle pianificazioni di aggiornamento di CA ARCserve Central Applications

È possibile impostare una pianificazione per il download automatico degli aggiornamenti di prodotto da un server CA oppure da un server di gestione temporanea software locale.

Per configurare le pianificazioni di aggiornamento di CA ARCserve Central Applications

1. Accedere all'applicazione.
2. Fare clic su Configurazione sulla barra di navigazione per aprire la schermata Configurazione.
3. Dal pannello di configurazione, fare clic su Configurazione aggiornamento.

   Verranno visualizzate le opzioni di configurazione degli aggiornamenti.
4. Selezionare un server di download.
   - **CA Server** - Fare clic su Impostazioni proxy per visualizzare le opzioni seguenti:
     - **Utilizza le impostazioni proxy del browser** - Consente di utilizzare le credenziali immesse per il proxy del browser.

       Nota: l'opzione Utilizza le impostazioni proxy del browser influisce sul funzionamento di Internet Explorer e Chrome.
     - **Configura impostazioni proxy** - Specificare l'indirizzo IP o il nome host del server proxy e il numero di porta. Se il server specificato richiede l'autenticazione, selezionare l'opzione Il server proxy richiede l'autenticazione e immettere le credenziali.

       Fare clic su OK per tornare alla configurazione aggiornamenti.
   - **Server di gestione temporanea** - Se si sceglie questa opzione, fare clic su Aggiungi server per aggiungere un server di gestione temporanea all'elenco. Immettere il nome host e il numero di porta del server, quindi fare clic su OK.

     Se si specificano più server di gestione temporanea, l'applicazione tenterà di utilizzare il primo server contenuto nell'elenco. Se la connection viene eseguita correttamente, i server restanti non verranno utilizzati per la gestione temporanea.
5. (Facoltativo) Per verificare la connessione del server, fare clic su Verifica connessione e attendere il completamento della verifica.
6. (Facoltativo) Fare clic Verifica aggiornamenti automaticamente e specificare il giorno e l'ora desiderati. La pianificazione può essere effettuata su base giornaliera o settimanale.

Fare clic su Salva per applicare la configurazione di aggiornamento.

Configura impostazioni proxy

CA ARCserve Central Applications consente di specificare un server proxy per la comunicazione con il supporto tecnico di CA per verificare la disponibilità di aggiornamenti e scaricarli. Per attivare questa funzionalità, specificare il server proxy che si desidera impostare per la comunicazione del server CA ARCserve Central Applications.

Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Configurazione sulla barra di spostamento.

   Verranno visualizzate le opzioni di configurazione.

2. Fare clic su Configurazione aggiornamento.

   Verrà visualizzata la finestra di dialogo Configurazione aggiornamento.

3. Fare clic su Impostazioni proxy.

   Verrà visualizzata la finestra di dialogo Impostazioni proxy.

4. Selezionare una delle seguenti opzioni:

   - **Utilizza le impostazioni proxy del browser** - Consente all'applicazione di rilevare e utilizzare le stesse impostazioni proxy applicate al browser per connettersi al server di CA Technologies per aggiornare le informazioni.

     Nota: questo comportamento è valido solo per i browser Internet Explorer e Chrome.

   - **Configura impostazioni proxy** - Consente di definire un server alternativo che l'applicazione utilizzerà per comunicare con il Supporto tecnico di CA per verificare la disponibilità di aggiornamenti. Il server alternativo (proxy) garantisce protezione e migliora le prestazioni e il controllo amministrativo.

     Completare i seguenti campi:

     – **Server proxy** - Specificare il nome host o l'indirizzo IP del server proxy.

     – **Porta** - Specificare il numero di porta che il server proxy utilizzerà per comunicare con il sito Web del Supporto tecnico di CA.

     – **(Facoltativo) Il server proxy richiede l'autenticazione -** Se le credenziali di accesso per il server proxy non sono uguali a quelle per il server CA ARCserve Central Applications, selezionare la casella di controllo Il server proxy richiede l'autenticazione e specificare il nome utente e la password per l'accesso al server proxy.

       Nota: per specificare il nome utente utilizzare il formato <nome dominio>/<nome utente>.

   Fare clic su OK.

Le impostazioni proxy sono configurate.

Configurazione delle preferenze di Social network

CA ARCserve Central Applications consente di gestire gli strumenti di Social network che possono agevolare la gestione delle singole applicazioni. È possibile generare newsfeed, specificare collegamenti a siti Web di social network popolari e selezionare siti Web video.

Per configurare le preferenze di Social network

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, selezionare Configurazione.

   Verrà visualizzata la finestra di dialogo Configurazione.

2. Dal pannello Configurazione, fare clic su Configurazione delle preferenze.

   Vengono visualizzate le opzioni relative alle preferenze.

3. Specificare le opzioni desiderate:

   - **Newsfeed** - L'applicazione visualizza i feed RSS relativi alle notizie più recenti di CA ARCserve Central Applications e CA ARCserve D2D e le informazioni sui prodotti dal Centro di consultazione esperti. I feed verranno visualizzati nella pagina principale.
   - **Social network** - L'applicazione visualizza nella pagina principale le icone di accesso a Twitter e Facebook per i siti Web di social network relativi a CA ARCserve Central Applications e CA ARCserve D2D.
   - **Video** - Consente di selezionare il tipo di video per la visualizzazione dei prodotti CA ARCserve Central Applications e CA ARCserve D2D (Impostazione predefinita: Video di YouTube).

   Fare clic su Salva.

   Le opzioni di Social network verranno applicate

4. Dalla barra di navigazione fare clic su pagina iniziale.

   Verrà visualizzata la pagina iniziale.

5. Aggiornare il browser.

   Le opzioni di Social network verranno applicate.

Modificare l'account di amministratore

CA ARCserve Central Applications consente di modificare il nome utente e/o la password per l'account dell'amministratore dopo l'installazione dell'applicazione. L'account di amministratore viene utilizzato solo per il nome utente predefinito visualizzato sulla schermata di accesso.

Nota: il nome utente specificato deve essere un account amministrativo di Windows o un account che dispone di privilegi di amministratore di Windows.

Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Configurazione sulla barra di spostamento.

   Vengono visualizzate le opzioni di configurazione.

2. Fare clic su Account di amministratore

3. Vengono visualizzate le impostazioni dell'account di amministratore.

4. Aggiornare i seguenti campi:

   - Nome utente
   - Password

   Fare clic su Salva.

L'account di amministratore viene modificato.

Configurazione delle impostazioni di distribuzione di D2D

CA ARCserve Central Protection Manager consente di configurare le impostazioni di distribuzione di D2D in base alla posizione in cui si desidera distribuire CA ARCserve D2D.

Nota: per effettuare la distribuzione di CA ARCserve D2D su computer in cui è in esecuzione Windows XP, disattivare l'opzione Utilizza condivisione file semplice del computer remoto Windows XP.

Per configurare le impostazioni di distribuzione di D2D

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, selezionare Configurazione.

   Verrà visualizzata la schermata Configurazione.

2. Nel riquadro Configurazione, fare clic su Configurazione della distribuzione D2D.

   Verranno visualizzate le opzioni di configurazione della distribuzione di D2D.

3. Completare i campi seguenti della schermata di configurazione:

   - **Porta** - Questo numero di porta viene utilizzato per la connessione all'interfaccia utente basata sul Web. Per impostazione predefinita, il numero di porta è 8014.
   - **Percorso di installazione** - Si tratta del percorso di installazione sul server remoto per CA ARCserve D2D. Il percorso predefinito è %Programmi%.
   - **Consenti al programma di installazione di installare il driver** (selezionato per impostazione predefinita) - Specificare se si desidera che il driver venga installato automaticamente.
   - **Riavvia** (impostazione predefinita: Sì) - Consente di specificare se si desidera eseguire il riavvio automatico al completamento del processo di distribuzione oppure se si desidera riavviare il sistema manualmente in un secondo momento.
   - **Usa HTTPS** (impostazione predefinita: No) - HTTPS (protetto) fornisce un livello di protezione superiore rispetto alla comunicazione HTTP. Il protocollo di comunicazione HTTPS è consigliato se si trasmettono informazioni riservate sulla rete.

4. Fare clic su Salva.

La configurazione di distribuzione di D2D viene applicata.

Configurazione del database

Dopo aver installato CA ARCserve Central Protection Manager è possibile eseguire le seguenti operazioni:

- Aggiornare le impostazioni per il database CA ARCserve Central Protection Manager. Ad esempio, è possibile aggiornare il nome dell'istanza, i valori della porta e così via.
- Modificare l'applicazione di database CA ARCserve Central Protection Manager a Microsoft SQL Server.
- Modificare l'applicazione di database CA ARCserve Central Protection Manager a Microsoft SQL Server Express Edition.

Per configurare il database CA ARCserve Central Protection Manager

1. Dalla barra di navigazione, fare clic su Configurazione.
2. Dal pannello di Configurazione, fare clic su Configurazione database.
3. Completare i campi seguenti della schermata di configurazione:
   - **Nome del computer SQL Server** - Specificare il nome del server che ospita l'istanza SQL Server.
   - **Istanza SQL Server** - Specificare il nome dell'istanza SQL Server.
   - **Porta SQL Server** - Specificare il numero di porta di questa istanza o abilitare l'opzione di rilevamento automatico.
   - **Modalità di autenticazione** - La modalità predefinita è la Modalità di autenticazione Windows.

     Nota: selezionando SQL Server e Modalità di autenticazione Windows verranno abilitati i campi Nome utente e Password.
   - (Facoltativo) **Test** - Fare clic sul Test per verificare la comunicazione tra l'applicazione e l'istanza di Microsoft SQL Server.
   - **Specificare i valori del Pool di connessioni di database** - Il valore minimo consentito è 1 e quello massimo 99.
4. Fare clic su Salva.

   Nota: fare clic su Reimposta per deselezionare tutti i valori specificati e caricare i dati originali.
5. (Facoltativo) Se l'applicazione fornisce dati a CA ARCserve Central Reporting, aprire Server Manager di Windows e riavviare il seguente servizio:

   `Servizio CA ARCserve Central Applications`

   La configurazione del server di database verrà applicata.

Ricreazione del database CA ARCserve Central Protection Manager

Per diversi motivi, potrebbe essere necessario ricreare il database CA ARCserve Central Protection Manager. Ad esempio, nel caso in cui il database contenga più di 10GB di dati. Nella procedura seguente viene descritto come ricreare il database CA ARCserve Central Protection Manager. La procedura viene applicata ai database Microsoft SQL Server e Microsoft SQL Server Express Edition.

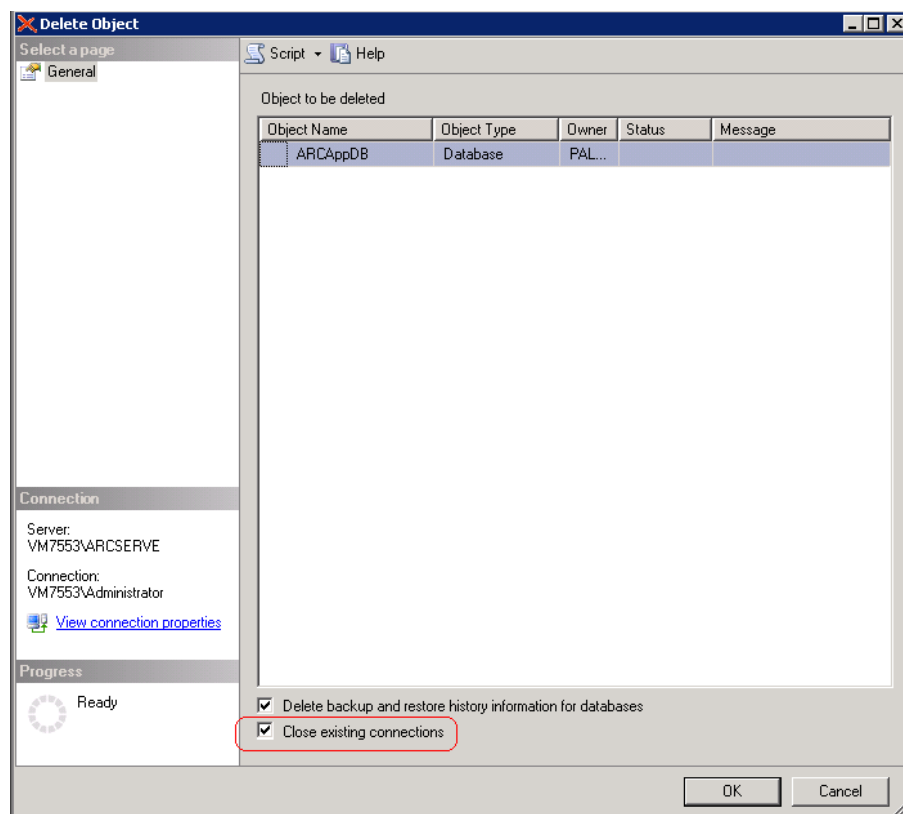
Importante: Se il database CA ARCserve Central Protection Manager viene eliminato, tutti i dati correnti andranno persi.

Per ricreare il database CA ARCserve Central Protection Manager

1. Aprire Microsoft SQL Server Management Studio Express e accedere all'istanza ARCserve_APP.

   Nota: se Microsoft SQL Server Management Studio Express non è installato sul server CA ARCserve Central Protection Manager, è possibile scaricare l'utilità dall'Area download di Microsoft.

2. Fare clic con il tasto destro del mouse su ARCAppDB, quindi selezionare Elimina dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Elimina oggetto.

3. Fare clic su Chiudi connessioni esistenti, quindi selezionare OK.

   La finestra di dialogo Elimina oggetto verrà chiusa e il database CA ARCserve Central Protection Manager verrà eliminato.

4. Aprire CA ARCserve Central Protection Manager e fare clic su Configurazione della barra di navigazione.

   Verranno visualizzate le opzioni di configurazione.

5. Fare clic su Configurazione database.

   Vengono visualizzate le opzioni del database.

6. Verificare la validità dei valori specificati nei seguenti campi:
   - **Nome del computer SQL Server** - Specificare il nome del server che ospita l'istanza SQL Server.
   - **Istanza SQL Server** - Specificare il nome dell'istanza SQL Server.
7. (Facoltativo) Completare i seguenti campi:
   - **Porta SQL Server** - Specificare il numero di porta di questa istanza o abilitare l'opzione di rilevamento automatico.
   - **Modalità di autenticazione** - La modalità predefinita è la Modalità di autenticazione Windows.

     Nota: selezionando SQL Server e Modalità di autenticazione Windows verranno abilitati i campi Nome utente e Password.
   - **Specificare i valori del Pool di connessioni di database** - Il valore minimo consentito è 1 e quello massimo 99.
8. Fare clic su Verifica per stabilire la connessione con il database.
9. Fare clic su Salva.

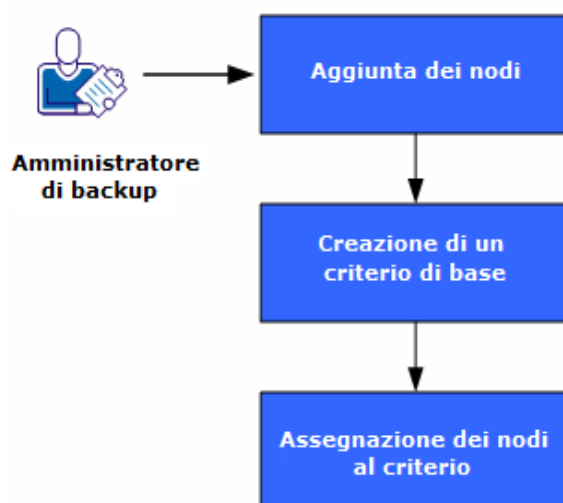
Il database verrà ricreato da CA ARCserve Central Protection Manager. Il nome dell'istanza di database corrisponderà a ARCAppDB.

Capitolo 4: Utilizzo di CA ARCserve Central Protection Manager

Questa sezione contiene i seguenti argomenti:

Utilizzo di CA ARCserve Central Protection Manager per il backup dei nodi CA ARCserve D2D

È possibile utilizzare CA ARCserve Central Protection Manager per creare criteri che consentono di definire la modalità e i tempi di esecuzione del backup e dell'archiviazione dei dati sui nodi CA ARCserve D2D. Le informazioni contenute negli argomenti seguenti descrivono le modalità di inoltro dei processi di backup di CA ARCserve D2D utilizzando un criterio di base. I criteri di base consentono di proteggere la maggior parte dei nodi di CA ARCserve D2D utilizzati in ambienti di produzione.

Il diagramma seguente mostra il processo utilizzato per creare un criterio di backup di base ed eseguire il backup dei nodi CA ARCserve D2D con CA ARCserve Central Protection Manager:

Per utilizzare CA ARCserve Central Protection Manager per creare un criterio di base ed eseguire il backup dei nodi CA ARCserve D2D, effettuare le operazioni seguenti:

1. Aggiungere i nodi (a pagina 53).
2. Creare un criterio di base (a pagina 53).
3. Assegnare i nodi a un criterio (a pagina 58).

Aggiunta di nodi

Per poter eseguire il backup dei nodi CA ARCserve D2D mediante un criterio, è necessario definire i nodi di cui si desidera eseguire il backup.

Nota: la procedura di rilevamento consente di automatizzare questa attività. Tuttavia, il rilevamento individua solamente i nodi presenti in Active Directory o sui server Active Directory.

Procedere come descritto di seguito:

1. Eseguire l'accesso a CA ARCserve Central Protection Manager e fare clic su Nodo nella barra di navigazione.
2. Dalla barra degli strumenti Nodo, fare clic su clic Aggiungi, quindi selezionare Aggiungi nodo per IP/Nome dal menu di scelta rapida.
3. Completare tutti i capi della finestra di dialogo Aggiungi nodo per IP/Nome e fare clic su OK.
4. (Facoltativo) Se il nodo aggiunto non compare nell'elenco dei nodi, fare clic su Aggiorna nella barra degli strumenti Nodo.

   Nota: per aggiungere altri nodi, ripetere i passaggi 2, 3, e 4.

Una volta aggiunto il nodo, questo verrà visualizzato nei gruppi predefiniti.

Creazione di un criterio di base

I criteri consentono di definire le modalità e i tempi di esecuzione del backup e dell'archiviazione dei dati presenti sui nodi CA ARCserve D2D.
CA ARCserve Central Protection Manager non include criteri predefiniti. La creazione di un criterio è un'attività preliminare per l'esecuzione del backup dei dati presenti sui nodi.

Per creare un criterio di base, specificare le impostazioni di protezione e creare una pianificazione. Le impostazioni di protezione definiscono i dati da includere nel backup, nonché il percorso e la modalità di archiviazione dei dati. La pianificazione definisce la data e la frequenza del backup dei nodi.

Procedere come descritto di seguito:

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri dalla barra di navigazione per accedere alla schermata Criteri.
2. Fare clic su Nuovo per creare un nuovo criterio.
3. Nel campo Nome criterio della finestra di dialogo Nuovo criterio, specificare un nome per il criterio.

4. Fare clic sulla scheda Impostazioni di backup e selezionare Impostazioni di protezione per visualizzare le opzioni di impostazione della protezione.

5. Specificare la destinazione di backup.

   È possibile specificare un percorso locale (volume o cartella) oppure una cartella condivisa remota (o unità mappata) come posizione di backup.

   - Se si sceglie di eseguire il backup in un percorso locale (volume o cartella), la destinazione di backup specificata non deve coincidere con il percorso di origine del backup. Nel caso in cui l'origine sia stata inclusa inavvertitamente nella destinazione, tale parte dell'origine verrà esclusa dal backup.

     Importante. Verificare che il volume di destinazione specificato non contenga informazioni di sistema. CA ARCserve D2D non esegue il backup dei volumi di destinazione contenenti informazioni di sistema. Se si tenta di eseguire il recupero del computer mediante il ripristino bare metal (BMR), potrebbe verificarsi un errore dell'operazione.

     Nota: non è possibile eseguire il recupero di dischi dinamici a livello del disco. Se il backup dei dati viene eseguito su un volume che risiede su un disco dinamico, tale disco non potrà essere ripristinato durante il ripristino bare metal.

   - In caso di backup dei dati in una posizione condivisa remota, specificare un percorso e le credenziali richieste per l'accesso al computer remoto.

6. Specificare l'origine di backup.

   È possibile impostare il backup dell'intero computer oppure di un singolo volume del nodo.

   Tenere presenti le seguenti considerazioni:

   - Se l'opzione di backup completo del computer è stata selezionata, CA ARCserve D2D rileva automaticamente i volumi/dischi collegati al computer e li include nel backup.

   - Se il volume di sistema/avvio non viene selezionato per il backup, verrà visualizzato un messaggio di avviso. Il messaggio indica che non è possibile utilizzare il backup per il ripristino bare metal.

7. Specificare i punti di ripristino.

   Specificare la quantità di immagini di backup memorizzate. Il valore predefinito è 31 e il valore massimo consentito è 1344. In caso di modifica di questa quantità, considerare lo spazio libero disponibile sulla destinazione.

   Se la quantità di punti di ripristino specificata viene superata, CA ARCserve D2D unisce il primo backup incrementale figlio con il backup padre, creando una nuova immagine di base. La nuova immagine di base è costituita dal blocco del backup padre più il blocco del primo backup incrementale figlio. Il ciclo di unione del primo backup figlio con il backup padre viene ripetuto per ciascun backup successivo. Questo processo consente di eseguire un numero infinito di backup incrementali senza modificare il valore di memorizzazione.

8. Specificare il tipo di compressione da utilizzare per i backup.

   La compressione riduce l'utilizzo dello spazio su disco ma produce un impatto inverso sulla velocità di backup a causa del maggior utilizzo della CPU.

   Di seguito sono riportate le opzioni di compressione disponibili:

   Nessuna compressione

   Non verrà eseguita alcuna compressione. L'opzione determina un utilizzo minimo della CPU (velocità massima) e un utilizzo massimo dello spazio su disco per la creazione dell'immagine di backup.

   Compressione standard

   Verrà eseguito un certo livello di compressione. Questa opzione fornisce un buon bilanciamento tra l'utilizzo della CPU e dello spazio su disco. Per impostazione predefinita viene utilizzata la compressione standard.

   Compressione massima

   Verrà eseguita la compressione massima. L'opzione implica un utilizzo massimo di CPU (velocità minima) ma utilizza anche una quantità minore di spazio su disco per l'immagine di backup.

   Tenere presenti le seguenti considerazioni:

   - Se l'immagine di backup contiene dati non comprimibili, quali immagini JPG, file ZIP ecc., sarà necessario allocare ulteriore spazio di archiviazione per la gestione di tali dati.
   - Se la destinazione non dispone di sufficiente spazio libero, è possibile aumentare il livello di compressione del backup.

9. Specificare le impostazioni di crittografia che si desidera utilizzare per la protezione aggiuntiva.

   a. Selezionare il tipo di algoritmo di crittografia da utilizzare per i backup.

      La crittografia dei dati corrisponde alla conversione di dati in un modulo incomprensibile senza un meccanismo di decifratura. La protezione dei dati di CA ARCserve D2D utilizza algoritmi di crittografia AES (Advanced Encryption Standard) per ottenere la massima protezione e riservatezza dei dati.

      Le opzioni di formato disponibili sono Nessuna crittografia, AES-128, AES-192 e AES-256. Per disattivare l'opzione di crittografia, selezionare Nessuna crittografia.

      - Il backup completo e i backup incrementali e di verifica correlati devono utilizzare lo stesso algoritmo di crittografia.
      - Nel caso in cui l'algoritmo di crittografia per un backup incrementale o di verifica venga modificato, sarà necessario eseguire un backup completo. In seguito alla modifica dell'algoritmo di crittografia, la prima esecuzione del backup sarà di tipo completo, indipendentemente dal tipo di backup impostato.

        Ad esempio, se si modifica il formato dell'algoritmo e si procede all'invio manuale di un backup incrementale o di verifica personalizzato, il backup si converte automaticamente in backup completo.

   b. Dopo aver specificato un algoritmo di crittografia, è necessario specificare e confermare una password di crittografia.

      - La password di crittografia può contenere un massimo di 23 caratteri.
      - Il backup completo e i relativi backup incrementali e di verifica devono utilizzare la stessa password di crittografia.
      - Nel caso in cui la password di crittografia per un backup incrementale o di verifica venga modificata, sarà necessario eseguire un backup completo. In seguito alla modifica della password di crittografia, la prima esecuzione del backup sarà di tipo completo, indipendentemente dal tipo di backup impostato.

        Ad esempio, se si modifica la password di crittografia e si procede all'invio manuale di un backup incrementale o di verifica personalizzato, il backup si converte automaticamente un backup completo.

   Se la crittografia viene abilitata, il registro attività viene aggiornato per descrivere la crittografia utilizzata per ciascun backup.

10. Specificare il limite di velocità del backup.

    È possibile specificare la velocità massima di scrittura (MB/min) del backup e limitare la velocità di backup per ridurre l'utilizzo della CPU o della rete. Tuttavia, la limitazione della velocità di backup potrebbe influire sul tempo di completamento del backup.

11. Fare clic sulla scheda Pianificazione per visualizzare le opzioni corrispondenti.

12. Specificare la pianificazione di backup:

    Imposta data e ora di inizio

    Specifica la data e l'ora di inizio dei backup pianificati.

    Backup incrementale

    Specifica la pianificazione dei backup incrementali.

    Le opzioni disponibili sono Ripeti e Mai. Se si seleziona l'opzione Ripeti, è necessario specificare l'intervallo di tempo (in minuti, ore o giorni) tra i tentativi di backup. L'intervallo minimo per l'esecuzione di un backup incrementale è di 15 minuti.

    Per impostazione predefinita, la pianificazione dei backup incrementali è impostata con cadenza giornaliera.

    Backup completo

    Specifica la pianificazione dei backup completi.

    CA ARCserve D2D esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base alla pianificazione specificata. Le opzioni disponibili sono Ripeti e Mai. Se si seleziona l'opzione Ripeti, è necessario specificare l'intervallo di tempo (in minuti, ore o giorni) tra i tentativi di backup. L'intervallo minimo per l'esecuzione di un backup completo è di 15 minuti.

    Per impostazione predefinita, la pianificazione per i backup completi è impostata su Mai (nessuna ripetizione pianificata).

    Backup di verifica

    Specifica la pianificazione dei backup di verifica.

    Le opzioni disponibili sono Ripeti e Mai. Se si seleziona l'opzione Ripeti, è necessario specificare l'intervallo di tempo (in minuti, ore o giorni) tra i tentativi di backup. L'intervallo minimo per l'esecuzione di un backup di verifica è di 15 minuti.

    Per impostazione predefinita, la pianificazione per i backup di verifica è impostata su Mai (nessuna ripetizione pianificata).

13. Fare clic su Salva.

Il criterio di backup di base viene creato. Il criterio viene visualizzato nell'elenco dei criteri con il nome specificato nella Fase 3 della schermata Criteri.

Nota: in caso di pianificazione simultanea di più tipi di backup, l'ordine di esecuzione verrà stabilito in base alle seguenti priorità:

- Priorità 1 - Backup completo
- Priorità 2 - Backup di verifica
- Priorità 3 - Backup incrementale

Esempio: se la pianificazione prevede l'esecuzione simultanea dei tre i tipi di backup, CA ARCserve D2D eseguirà il backup completo. Se la pianificazione prevede l'esecuzione simultanea di un backup di verifica e di un backup incrementale ma non di un backup completo, CA ARCserve D2D eseguirà il backup di verifica. Il backup incrementale pianificato verrà eseguito solo nel caso in cui non esista alcun conflitto con un altro tipo di backup.

Assegnazione di nodi a un criterio

Dopo avere creato il criterio di base, assegnare al criterio i nodi di CA ARCserve D2D di cui si desidera eseguire il backup.

Procedere come descritto di seguito:

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri dalla barra di navigazione per accedere alla schermata Criteri.
2. Selezionare il criterio creato dall'elenco dei criteri della schermata Criterio.
3. Fare clic sulla scheda Assegnazione criterio per visualizzare l'elenco di assegnazione dei criteri.
4. Fare clic su Assegnazione e annullamento assegnazione per accedere alla finestra di dialogo Assegna/Annulla assegnazione criterio.
5. Selezionare la casella di controllo accanto ai nodi che si desidera aggiungere, quindi fare clic sulla freccia destra.

   Verrà visualizzata la finestra di dialogo Contratto di licenza.

6. Leggere e accettare i termini del contratto di licenza, quindi fare clic su Completato.

   I nodi verranno assegnati al criterio creato e distribuiti immediatamente. Il backup viene avviato in base alla pianificazione definita nella scheda Pianificazione.

7. Una volta completata l'assegnazione dei nodi ai criteri, fare clic su OK per salvare e chiudere la finestra di dialogo Assegnazione e annullamento assegnazione.

Una volta completata l'assegnazione dei criteri,
CA ARCserve Central Protection Manager esegue la distribuzione del criterio sui nodi. Le operazioni di backup vengono avviate in base alle impostazioni di protezione selezionate e alla pianificazione definita nel criterio.

Modalità di gestione dei nodi in CA ARCserve Central Protection Manager

CA ARCserve Central Protection Manager fornisce diversi strumenti e opzioni per la gestione di nodi e gruppi di nodi. Questa sezione include informazioni sulle modalità di eliminazione, aggiunta, modifica e sincronizzazione di nodi e gruppi di nodi. È possibile eseguire il rilevamento e la distribuzione di CA ARCserve D2D sui nodi.

In questa sezione verranno illustrati i seguenti argomenti:

Informazioni sulla schermata di gestione dei nodi

La gestione dei nodi è un componente di CA ARCserve Central Applications. È possibile accedere a questa schermata dalla barra di navigazione disponibile nel riquadro sinistro dell'applicazione CA ARCserve Central Protection Manager.

Nella schermata di gestione dei nodi sono disponibili quattro categorie:

- **Nodo** - Consente di gestire nodi specifici. Per ulteriori informazioni sulla gestione dei nodi, consultare la sezione Operazioni possibili sui nodi (a pagina 62).
- **Gruppo nodi** - Consente di gestire gruppi di nodi specifici. Per ulteriori informazioni, consultare la sezione Operazioni possibili sui gruppi di nodi (a pagina 78).

- **Azioni** - Consente di eseguire ilbackup (a pagina 141), il ripristino (a pagina 145) e la distribuzione dei dati (a pagina 84).
- **Filtro** - Consente di utilizzare filtri per visualizzare i nodi in un gruppo su cui è installata una determinata applicazione. Per ulteriori informazioni, consultare la sezione Filtraggio di gruppi di nodi (a pagina 87).

Lo stato di ogni nodo riportato nella colonna Prodotti identifica le icone CA ARCserve Backup e CA ARCserve D2D. La tabella seguente descrive gli stati per ciascun prodotto della colonna Prodotto:

Icona	Descrizione
	Questo stato contrassegnato con la lettera M indica che il nodo corrisponde a un server primario o standalone di CA ARCserve Backup gestito da CA ARCserve Central Applications.
	Questo stato contrassegnato con la lettera M e un punto esclamativo nella parte inferiore destra, indica che il nodo corrisponde a un server primario o standalone di CA ARCserve Backup gestito da CA ARCserve Central Applications per il quale non è stata eseguita la sincronizzazione durante le ultime xx ore. Per impostazione predefinita xx corrisponde a un periodo di 48 ore oppure la sincronizzazione non è ancora stata eseguita.
	Questo stato senza la lettera M indica che il nodo corrisponde a un server CA ARCserve Backup primario, standalone o membro non gestito da CA ARCserve Central Applications.
	Lo stato indica che il nodo contiene una versione precedente di CA ARCserve Backup
	Questo stato indica che il nodo non è gestito da CA ARCserve Central Applications e non può stabilire la connessione a CA ARCserve D2D.
	Lo stato indica che il nodo contiene una versione precedente di CA ARCserve D2D.
	Questo stato contrassegnato con la lettera M indica che il nodo è gestito da CA ARCserve Central Applications ed è connesso a CA ARCserve D2D.
	Questo stato contrassegnato con la lettera M indica che il nodo è gestito da CA ARCserve Central Applications e non è connesso a CA ARCserve D2D.
	Questo stato contrassegnato con la lettera M indica che il nodo è gestito da CA ARCserve Central Applications ed è connesso a CA ARCserve D2D con avvisi.
	Questo stato contrassegnato con la lettera M e un punto esclamativo nella parte inferiore destra indica che il nodo corrisponde a un server CA ARCserve D2D gestito da CA ARCserve Central Applications per il quale non è stata eseguita la sincronizzazione durante le ultime xx ore. Per impostazione predefinita xx corrisponde a un periodo di 48 ore oppure la sincronizzazione non è ancora stata eseguita.

Operazioni possibili sui nodi

CA ARCserve Central Protection Manager consente di aggiungere, modificare ed eliminare i nodi, di eseguire la sincronizzazioni dei dati, definire le impostazioni per i nodi, esportare le informazioni sul nodo in formato CSV e determinare lo stato di ciascun nodo.

Nota: quando a CA ARCserve Central Protection Manager vengono aggiunti nodi corrispondenti a server CA ARCserve Backup e CA ARCserve D2D e viene effettuata una sincronizzazione su ciascun nodo, i dati del nodo vengono generati e possono essere visualizzati in CA ARCserve Central Reporting. Per ulteriori informazioni sulla sincronizzazione, consultare la sezione Dati e opzioni di sincronizzazione (a pagina 73).

Aggiunta di nodi mediante il rilevamento

CA ARCserve Central Protection Manager consente di aggiungere più nodi mediante il processo di rilevamento.

Per aggiungere nodi mediante il rilevamento:

1. Accedere all'applicazione e fare clic su Nodi nella barra di navigazione.

   Verrà visualizzata la schermata Nodi.

2. Fare clic su Rileva nella barra degli strumenti Nodo.

   Verrà visualizzata la finestra di dialogo Rileva nodi mediante Active Directory.

3. Completare i seguenti campi:

   - Nome utente (Dominio)
   - Password (Dominio)
   - Filtro nome computer

   Fare clic su Aggiungi e quindi su Avvia rilevamento.

   Viene eseguito il rilevamento. (a pagina 63)

4. Una volta completato il processo di rilevamento dei nodi, verrà visualizzato il messaggio seguente:

   `Continuare ad aggiungere nodi dai risultati di rilevamento?`

   Fare clic su Sì per accedere a Aggiungi nodi dai risultati di rilevamento.

   Nota: per chiudere il messaggio senza aggiungere nodi, fare clic su No.

   Verrà visualizzata la schermata Aggiungi nodi dai risultati di rilevamento contenente un elenco dei nodi rilevati.

5. Dall'elenco Nodi rilevati, selezionare i nodi che si desidera aggiungere, quindi fare clic sulla freccia per aggiungerli all'elenco Nodi da proteggere. Al termine della procedura fare clic su Avanti.

   Nota: è possibile filtrare l'elenco in base al nome del nodo o del dominio per ridurre l'elenco.

6. (Facoltativo) Selezionare uno o più nodi e fare clic su Nascondi nodi selezionati per nascondere i nodi di cui non si desidera eseguire il backup.

7. (Facoltativo) Selezionare l'opzione Mostra nodi nascosti per visualizzare nuovamente i nodi nascosti per l'elenco Nodi rilevati. Per nascondere nuovamente i nodi, deselezionare l'opzione.

8. Nella schermata Credenziali nodo, immettere un nome utente e una password per il nodo che si desidera aggiungere. È possibile specificare credenziali globali oppure utilizzare credenziali specifiche per i nodi selezionati.

9. Fare clic su Fine.

I nodi verranno aggiunti.

Finestra di dialogo Monitor di rilevamento

La finestra di dialogo Monitor di rilevamento visualizza lo stato generale dei nodi rilevati nell'ambiente dell'utente

e contiene le seguenti informazioni:

Fase

Visualizza le tre fasi di rilevamento dei nodi: Rilevamento nodo, Aggiornamento dei dati e Rilevamento completato.

Stato

Visualizza uno stato Attivo durante il processo di rilevamento e uno stato Completato al termine del rilevamento.

Tempo trascorso

Visualizza il tempo impiegato per il rilevamento dei nodi.

Numero di nodi elaborati

Visualizza il numero di nodi elaborati registrato e aggiornato nel database.

Aggiunta di nodi per indirizzo IP o nome nodo

CA ARCserve Central Protection Manager consente di aggiungere i nodi CA ARCserve D2D e CA ARCserve Backup a un gruppo di nodi in base all'indirizzo IP o il nome host del nodo.

Per aggiungere nodi per indirizzo IP o nome nodo

1. Dalla pagina principale, selezionare Nodo nella barra di navigazione.

   Verrà visualizzata la schermata Nodo.

2. Dalla barra degli strumenti Nodo, fare clic su clic Aggiungi, quindi selezionare Aggiungi nodo per IP/Nome dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Aggiungi nodo per IP/Nome.

3. Completare i seguenti campi:

   - **IP/Nome nodo** - Consente di specificare l'indirizzo IP o il nome del nodo.
   - **Descrizione** - Consente di specificare una descrizione per il nodo.
   - **Nome utente** - Consente di specificare il nome utente richiesto per l'accesso al nodo.
   - **Password** - Consente di specificare la password richiesta per l'accesso al nodo.

   Fare clic su OK.

4. (Facoltativo) Se il nodo aggiunto non compare nell'elenco dei nodi, fare clic su Aggiorna nella barra degli strumenti.

   La finestra di dialogo Aggiungi nodo per IP/Nome verrà chiusa e il nodo verrà aggiunto.

5. (Facoltativo) Se CA ARCserve Backup viene installato sul nodo e le credenziali di CA ARCserve Central Protection Manager non dispongono dei privilegi di amministratore di CA ARCserve Backup, viene visualizzato il seguente messaggio:

   `È necessario disporre dei privilegi di amministratore di ARCserve Backup.`

   Per continuare, specificare le credenziali di accesso per l'account di amministratore di CA ARCserve Backup, quindi fare clic su OK.

   Nota: CA ARCserve Central Protection Manager può eseguire la sincronizzazione dei dati soltanto su server primari e stand-alone di CA ARCserve Backup. Quando il server primario è un server filiale, CA ARCserve Central Protection Manager è in grado di eseguire la sincronizzazione dei dati CA ARCserve Backup soltanto con il server Global Dashboard.

Il nodo verrà aggiunto.

Aggiunta di nodi dai risultati del rilevamento

Questa opzione consente di selezionare i nodi rilevati automaticamente in base alle impostazioni specificate nel pannello Configurazione rilevamento.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Nodi nella barra di navigazione per aprire la schermata Nodi.

2. Dalla categoria Nodo, fare clic su Aggiungi e selezionare Aggiungi nodi dai risultati di rilevamento dal menu di popup.

   Verrà visualizzata la schermata Aggiungi nodi dai risultati di rilevamento contenente un elenco dei nodi rilevati.

3. Dall'elenco Nodi rilevati, selezionare i nodi che si desidera aggiungere, quindi fare clic sulla freccia per aggiungerli all'elenco Nodi da proteggere. Al termine della procedura fare clic su Avanti.

   Nota: è possibile filtrare l'elenco in base al nome del nodo o del dominio per ridurre l'elenco.

4. (Facoltativo) Selezionare uno o più nodi e fare clic su Nascondi nodi selezionati per nascondere i nodi di cui non si desidera eseguire il backup.

5. (Facoltativo) Selezionare l'opzione Mostra nodi nascosti per visualizzare nuovamente i nodi nascosti per l'elenco Nodi rilevati. Per nascondere nuovamente i nodi, deselezionare l'opzione.

6. Nella schermata Credenziali nodo, immettere un nome utente e una password per il nodo che si desidera aggiungere. È possibile specificare credenziali globali oppure utilizzare credenziali specifiche per i nodi selezionati.

7. Fare clic su Fine.

I nodi verranno aggiunti.

Aggiunta di nodi mediante l'importazione di computer virtuali da ESX/VC

L'opzione Aggiungi nodo consente di individuare e aggiungere tutti i computer virtuali presenti sul server host ESX o vCenter specificato.

Nota: verranno rilevati solamente i computer virtuali che dispongono degli strumenti VMware.

Per aggiungere nodi mediante l'importazione di computer virtuali da ESX/VC

1. Accedere all'applicazione e fare clic su Nodi nella barra di navigazione.

   Verrà visualizzata la schermata Nodi.

2. Dalla barra degli strumenti Nodo, fare clic su Aggiungi e selezionare Importa computer virtuali da ESX/VC dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Rileva nodi.

3. Completare i seguenti campi della schermata Rileva nodi:

   - Host Server ESX o vCenter - Specifica l'hypervisor da analizzare.
   - Nome utente
   - Password
   - Porta
   - Protocollo

   Fare clic su Connetti.

   L'applicazione analizza l'hypervisor specificato.

4. Al termine dell'analisi, fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Credenziali nodo.

5. Nella finestra di dialogo Credenziali nodo, fornire un nome utente e una password globali per tutti i computer virtuali rilevati, quindi fare clic su Applica ai nodi selezionati

6. (Facoltativo) Fare clic su un computer virtuale per immettere le credenziali corrispondenti.

7. Fare clic su Fine.

I computer virtuali selezionati vengono aggiunti al gruppo di nodo.

Importare nodi da un file

CA ARCserve Central Protection Manager consente di importare uno o più nodi da un file. È possibile importare nodi da un file di testo di valori delimitati da virgole (.txt) o da un foglio di calcolo (.CSV).

Per eseguire l'importazione dei nodi da un file

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Dalla barra degli strumenti Nodo, fare clic su Aggiungi, quindi selezionare Importa nodi da file nel menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Seleziona nodi.

3. Fare clic su Sfoglia per specificare il file contenente i nodi da importare.

   Nota: è possibile specificare file di testo di valori delimitati da virgole (.txt) o da un foglio di calcolo (.CSV).

   Fare clic su Carica.

   I nomi dei nodi e i nomi utenti corrispondenti verranno visualizzati nella finestra di dialogo.

4. Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Credenziali nodo.

   Se il nome utente e la password immessi sono corretti, verrà visualizzato un segno di spunta verde nel campo Verificato. Se il nome utente e la password immessi non sono corretti, verrà visualizzato un punto esclamativo di colore rosso nel campo Verificato.

5. Eseguire una delle seguenti operazioni:

   - Per aggiungere i nodi, verificare che i nomi utenti e le password siano corretti. Per modificare le credenziali per un nodo specifico, fare clic sul campo Nome nodo.

     Verrà visualizzata la finestra di dialogo Convalida credenziali.

     Compilare i campi obbligatori nella finestra di dialogo Convalida credenziali e fare clic su OK.

   - Per applicare un nome utente e una password globale a tutti i nodi, completare i campi Nome utente e Password, quindi fare clic su Applica ai nodi selezionati.

     Il nome utente globale e la password globale verrà applicato a tutti i nodi.

   Fare clic su Fine.

I nodi verranno aggiunti.

Aggiornamento dei nodi

CA ARCserve Central Protection Manager consente di aggiornare le informazioni sui nodi aggiunti precedentemente. È necessario procedere all'aggiornamento dei nodi nei casi seguenti:

- **Tutti i nodi**
  - Quando viene installato un prodotto nuovo sul nodo dopo la registrazione del nodo su CA ARCserve Central Protection Manager.
  - Quando viene eseguito l'aggiornamento del nome utente o della password dopo la registrazione del nodo su CA ARCserve Central Protection Manager.
- **Nodi di CA ARCserve Backup**
  - Quando viene eseguito l'aggiornamento di un server filiale di CA ARCserve Backup a un server primario di CA ARCserve Backup.
  - Quando viene eseguito l'aggiornamento di un server primario centrale di CA ARCserve Backup a un server primario di CA ARCserve Backup dopo la registrazione del server primario centrale su CA ARCserve Central Protection Manager.

  Nota: quando vengono aggiunti o aggiornati nodi il cui funzionamento corrisponde a quello dei server di succursale di CA ARCserve Backup associati a un server principale centrale, il nome host del server principale centrale viene visualizzato in due punti della schermata Nodo. La prima posizione della schermata Nodo corrisponde al gruppo Tutti i nodi. Il nome completo del server viene visualizzato nel gruppo Tutti i nodi, indipendentemente dalla quantità di caratteri contenuti nel nome host del server. La seconda posizione della schermata Nodo corrisponde a Gruppi Global Dashboard. Se il nome host del server contiene più di 15 caratteri, tale viene troncato a 15 caratteri in Gruppi Global Dashboard.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Dalla barra Gruppi, fare clic sul gruppo di Tutti i nodi oppure sul nome del gruppo contenente i nodi che si desidera aggiornare.

   I nodi associati al gruppo verranno visualizzati nell'elenco dei nodi.

3. Fare clic sul nodo da aggiornare, quindi fare clic con il tasto destro del mouse su Aggiorna nodo dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Aggiorna nodo.

   Nota: per aggiornare tutti i nodi del gruppo di nodi, fare clic con il tasto destro del mouse sul nome del gruppo di nodi e selezionare Aggiorna nodo dal menu di scelta rapida.

4. Aggiornare i dettagli del nodo.

   Nota: per aggiornare nodi multipli dell'Elenco nodi, selezionare i nodi desiderati, fare clic con il tasto destro del mouse su qualsiasi nodo, quindi selezionare Aggiorna nodo dal menu di scelta rapida. Il nome utente e la password coincidono per i nodi selezionati. L'opzione Specifica nuove credenziali e la casella di controllo Acquisisci controllo del nodo sono selezionate per impostazione predefinita. È possibile specificare un nuovo nome utente e una nuova password per i nodi selezionati ed imporre al server la gestione dei nodi specificati. Inoltre, è possibile selezionare l'opzione Usa le credenziali esistenti per applicare il nome utente e la password correnti. I campi vengono disattivati.

5. Fare clic su OK.

   La finestra di dialogo Aggiorna nodo verrà chiusa e i nodi verranno aggiornati.

   Nota: quando vengono aggiornati uno più campi descritti nel passaggio precedente, viene visualizzata la finestra di dialogo Aggiorna nodo che consente di specificare ulteriori dettagli.

6. (Facoltativo) Se le informazioni aggiornate non compaiono nell'elenco dei nodi, fare clic su Aggiorna nella barra degli strumenti.

Il nodo verrà aggiornato.

Eliminazione dei nodi

CA ARCserve Central Protection Manager consente di eliminare nodi dall'ambiente.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Nodo sulla barra di navigazione per aprire la schermata Nodo.

2. Dalla barra Gruppi, fare clic sul gruppo di Tutti i nodi oppure sul nome del gruppo contenente il nodo da eliminare.

   I nodi associati al gruppo verranno visualizzati nell'elenco dei nodi.

3. Selezionare i nodi che si desidera eliminare, quindi fare clic su Elimina sulla barra degli strumenti.

   Verrà visualizzato un messaggio di conferma.

4. Eseguire una delle seguenti operazioni:

   - Fare clic su Sì per eliminare il nodo.

   Fare clic su No se non si desidera eliminare il nodo.

Esportazione dei nodi in un file

CA ARCserve Central Protection Manager consente di eseguire l'esportazione dei nodi dal gruppo nodi selezionato con le informazioni relative alle credenziali in un file CSV.

Per esportare i nodi in un file:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Selezionare un gruppo di nodi da esportare.

   Vengono visualizzati i nodi per il gruppo di nodi selezionato.

3. Fare clic su Esporta dalla barra degli strumenti Nodo.

   Viene visualizzato un messaggio indicante che il file CSV conterrà password che verranno visualizzate come testo normale.

   Fare clic su Sì per aprire o salvare i file CSV oppure fare clic su No per annullare l'operazione.

I nodi vengono esportati in un file CSV.

Accesso ai nodi CA ARCserve D2D

L'accesso ai nodi di CA ARCserve D2D può essere eseguito dalla pagina principale di CA ARCserve Central Protection Manager.

Per accedere ai nodi CA ARCserve D2D

1. Aprire l'applicazione e fare clic su Nodi sulla barra di spostamento.

   Verrà visualizzata la schermata Nodo.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Individuare e fare clic sul nodo a cui si desidera accedere, quindi su Accesso a D2D dal menu di scelta rapida.

   Nota: se non viene aperta una nuova finestra, verificare che le opzioni del browser non blocchino la visualizzazione di tutti i popup o di quelli del sito Web corrente.

L'utente è connesso al nodo CA ARCserve D2D.

Nota: è possibile che durante il primo accesso al nodo CA ARCserve D2D venga visualizzata una pagina HTML contenente un messaggio di avviso. Questo comportamento si verifica con l'utilizzo di Internet Explorer. Per risolvere il problema, chiudere Internet Explorer e ripetere il passaggio 3. Sarà quindi possibile accedere al nodo CA ARCserve D2D correttamente.

Aggiornamento di nodi e criteri dopo la modifica del nome host del server CA ARCserve Central Applications

Quando viene eseguita una modifica del nome host del server CA ARCserve Central Protection Manager, è necessario aggiornare i nodi e i relativi criteri. Tali attività sono necessarie per mantenere la relazione fra il server CA ARCserve Central Protection Manager e i nodi protetti da tale server. La tabella seguente descrive gli scenari possibili e le azioni applicabili a ciascuno scenario.

Scenario	Misura correttiva
Il nodo è stato aggiunto dopo la modifica del nome host del server CA ARCserve Central Protection Manager.	Non è richiesto alcun intervento.
Il nodo è stato aggiunto prima della modifica del nome host del server CA ARCserve Central Protection Manager, senza applicare criteri.	Aggiornare il nodo. Per ulteriori informazioni, consultare la sezione Aggiornamento dei nodi (a pagina 68).

Scenario	Misura correttiva
Il nodo è stato aggiunto prima della modifica del nome host del server CA ARCserve Central Protection Manager, senza applicare criteri.	Applicare nuovamente il criterio. Per ulteriori informazioni, consultare la sezione Distribuzione dei criteri (a pagina 139).

Opzioni del processo di unione

CA ARCserve Central Protection Manager consente di interrompere e riprendere i processi di unione per ogni nodo in qualsiasi momento. Il processo di interruzione e ripresa dei processi di unione non interessa i processi in corso.

Interruzione di un processo di unione su un nodo

CA ARCserve Central Protection Manager consente di interrompere un processo di unione su un nodo specifico.

Ad esempio, i processi di unione possono utilizzare risorse di sistema e causare un rallentamento dei processi di backup. Utilizzare l'opzione di interruzione per interrompere un processo di unione in corso in modo che i processi di backup in corso possano essere completati con la massima efficienza. Al completamento del backup, è possibile riprendere il processo di unione.

Procedere come descritto di seguito:

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri dalla barra di navigazione per accedere alla schermata Nodo.
2. Selezionare il gruppo di nodi contenente i nodi con processi di unione che si desidera interrompere.

   Verrà visualizzato un elenco di nodi per il gruppo selezionato.
3. Fare clic sui nodi contenenti i processi di unione che si desidera interrompere. Fare quindi clic con il tasto destro del mouse sui nodi selezionati, quindi selezionare Sospendi processo di unione dal menu di scelta rapida.

   Nota: per impostazione predefinita, l'opzione Sospendi processo di unione è disattivata. Quando il nodo esegue un processo di unione, in base a quanto indicato nella colonna Processo, l'opzione Sospendi processo di unione viene abilitata.

Il processo di unione del nodo selezionato viene interrotto e può essere verificato dalla pagina principale di CA ARCserve D2D.

Ripresa di un processo di unione su un nodo

CA ARCserve Central Protection Manager consente di riprendere i processi di unione interrotti per nodi specifici.

Procedere come descritto di seguito:

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri dalla barra di navigazione per accedere alla schermata Nodo.
2. Selezionare il gruppo di nodi contenente i nodi con processi di unione che si desidera riprendere.

   Verrà visualizzato un elenco di nodi per il gruppo selezionato.
3. Fare clic sui nodi con processi di unione interrotti che si desidera riprendere. Fare quindi clic con il tasto destro del mouse sui nodi selezionati, quindi selezionare Riprendi processo di unione dal menu di scelta rapida.

   Nota: l'opzione Riprendi processo di unione è abilitata se non è in esecuzione un processo di backup e i processi di unione sono interrotti.

Il processo di unione del nodo selezionato viene ripreso e può essere verificato dalla pagina principale di CA ARCserve D2D.

Dati e opzioni di sincronizzazione

CA ARCserve Central Protection Manager consente di effettuare sincronizzazioni dei dati per ciascun nodo inviando le informazioni da un server primario CA ARCserve Backup (asdb) o da un database primario centrale di CA ARCserve D2D o di Global Dashboard (central_asdb) al database CA ARCserve Central Protection Manager (ARCAppDB).

La sincronizzazione dei dati garantisce la coerenza e l'aggiornamento dei dati nei diversi database affinché il database del sito centrale contenga le stesse informazioni presenti in ciascuno dei database registrati del sito della diramazione.

In questa sezione verranno illustrati i seguenti argomenti:

Sincronizzazione completa dei dati di CA ARCserve Backup per un nodo specifico o un gruppo di nodi

CA ARCserve Central Protection Managerconsente di eseguire la sincronizzazione completa dei dati di CA ARCserve Backup su un nodo specifico o su un gruppo di nodi.

Durante un processo di sincronizzazione completa di CA ARCserve Backup, il modulo database CA ARCserve Backup viene interrotto per alcuni minuti. In tal modo non sarà possibile eseguire la registrazione delle informazioni relative ai processi di CA ARCserve Backup fino al completamento del processo di sincronizzazione del database.

Per eseguire la sincronizzazione completa dei dati di CA ARCserve Backup per un nodo specifico o un gruppo di nodi

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Nodo nella barra di navigazione.

   Verrà visualizzata la schermata Nodo.

2. Selezionare il gruppo di nodi contenente il nodo da sincronizzare.

   Verrà visualizzato un elenco di nodi per il gruppo selezionato.

3. Eseguire una delle seguenti operazioni:

   - Per un nodo specifico, selezionare il nodo di CA ARCserve Backup nella parte destra della sezione Gruppi e fare clic su Sincronizzazione completa di CA ARCserve Backup dal menu di scelta rapida o dal pulsante Sincronizza dati della barra degli strumenti Nodo.
   - Per un gruppo di nodi, fare clic con il tasto destro del mouse sul gruppo di nodi e selezionare Sincronizzazione completa di CA ARCserve Backup dal menu di scelta rapida.

CA ARCserve Central Protection Manager inoltra la sincronizzazione completa dei dati di CA ARCserve Backup per il nodo o il gruppo di nodi selezionato.

Sincronizzazione incrementale dei dati di CA ARCserve Backup per un nodo o gruppo di nodi

CA ARCserve Central Protection Manager consente di eseguire sincronizzazioni incrementali dei dati CA ARCserve Backup su un nodo specifico.

L'opzione Sincronizzazione incrementale di CA ARCserve Backup sincronizza i dati modificati, eliminati o aggiunti in seguito all'ultima sincronizzazione. I dati sincronizzati vengono compressi in modo da ridurre al minimo le dimensioni prima della trasmissione.

Per eseguire la sincronizzazione incrementale dei dati di CA ARCserve Backup per un nodo o un gruppo di nodi

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Nodo nella barra di navigazione.

   Verrà visualizzata la schermata Nodo.

2. Selezionare il gruppo di nodi contenente il nodo da sincronizzare.

   Verrà visualizzato un elenco di nodi per il gruppo selezionato.

3. Eseguire una delle seguenti operazioni:

   - Per un nodo specifico, selezionare il nodo di CA ARCserve Backup nella parte destra della sezione Gruppi e fare clic su Sincronizzazione incrementale di CA ARCserve Backup dal menu di scelta rapida o dal pulsante Sincronizza dati della barra degli strumenti Nodo.
   - Per un gruppo di nodi, fare clic con il tasto destro del mouse sul gruppo di nodi e selezionare Sincronizzazione incrementale di CA ARCserve Backup dal menu di scelta rapida.

CA ARCserve Central Protection Manager inoltra la sincronizzazione incrementale dei dati di CA ARCserve Backup per il nodo o il gruppo di nodi selezionato.

Sincronizzazione completa dei dati di CA ARCserve D2D per un nodo specifico o un gruppo di nodi

CA ARCserve Central Protection Managerconsente di eseguire la sincronizzazione completa dei dati di CA ARCserve D2D su un nodo specifico o su un gruppo di nodi.

Per eseguire la sincronizzazione completa dei dati di CA ARCserve D2D per un nodo specifico o un gruppo di nodi

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Nodo nella barra di navigazione.

   Verrà visualizzata la schermata Nodo.

2. Selezionare il gruppo di nodi contenente il nodo da sincronizzare.

   Verrà visualizzato un elenco di nodi per il gruppo selezionato.

3. Eseguire una delle seguenti operazioni:

   - Per un nodo specifico, selezionare il nodo di CA ARCserve D2D nella parte destra della sezione Gruppi e fare clic su Sincronizzazione completa di CA ARCserve D2D dal menu di scelta rapida o dal pulsante Sincronizza dati della barra degli strumenti Nodo.
   - Per un gruppo di nodi, fare clic con il tasto destro del mouse sul gruppo di nodi e selezionare Sincronizzazione completa di CA ARCserve D2D dal menu di scelta rapida.

CA ARCserve Central Protection Manager inoltra la sincronizzazione completa dei dati di CA ARCserve D2D per il nodo o il gruppo di nodi selezionato.

Impostazioni dei nodi

In CA ARCserve Central Protection Manager è possibile impostare una pianificazione locale per ciascun nodo primario centrale di Global Dashboard o di CA ARCserve Backup al fine di eseguire sincronizzazioni incrementali per ciascun nodo.

Pianificazione della sincronizzazione dati di CA ARCserve Backup

Le impostazioni di CA ARCserve Backup consentono di creare pianificazioni personalizzate per ciascun nodo.

per pianificare la sincronizzazione dei dati di CA ARCserve Backup

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Nodo nella barra di navigazione.

   Verrà visualizzata la schermata Nodo.

2. Nell'elenco dei gruppi, selezionare il gruppo di nodi a cui si desidera applicare l'impostazione di CA ARCserve Backup.

   Verrà visualizzato un elenco di nodi per il gruppo selezionato.

3. Selezionare il nodo a cui applicare l'impostazione, quindi fare clic su Pianificazione di sincronizzazione dati di CA ARCserve Backup dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Pianificazione della sincronizzazione dati di CA ARCserve Backup.

4. Selezionare una delle seguenti opzioni:

   - **Abilita** - Consente di specificare le opzioni di pianificazione compilando i campi Metodo di ripetizione e Ora pianificata.

     – Ogni (numero di giorni)

     – Ogni giorno della settimana selezionato

     – Ogni giorno del mese selezionato

   - **Disabilita** - Consente di non applicare alcuna impostazione.

   - **Usa impostazione globale** - Consente di applicare le impostazioni globali configurate nel modulo di configurazione di CA ARCserve Backup. Per ulteriori informazioni, consultare la sezione Pianificazione della sincronizzazione dati di CA ARCserve Backup.

5. Fare clic su OK.

Le impostazioni di CA ARCserve Backup vengono applicate.

Operazioni possibili sui gruppi di nodi

CA ARCserve Central Protection Manager permette di creare gruppi di nodi assegnando singoli nodi a ciascun gruppo e di modificare ed eliminare gruppi di nodi.

Nota: Le operazioni di modifica ed eliminazione sono consentite solo per i gruppi di nodi creati dall'utente.

Aggiunta di gruppi di nodi

I gruppi di nodi consentono di gestire un insieme di computer origine CA ARCserve D2D in base a caratteristiche comuni. Ad esempio, è possibile definire gruppi di nodi classificati in base al dipartimento che supportano: Contabilità, Marketing, Legale, Risorse umane, ecc.

L'applicazione contiene i seguenti gruppi di nodi:

- **Gruppi predefiniti:**
  - **Tutti i nodi** - Contiene tutti i nodi associati con l'applicazione.
  - **Nodi senza un gruppo** - Contiene tutti i nodi associati all'applicazione non assegnati a un gruppo di nodi.
  - **Nodi senza un criterio** - Contiene tutti i nodi associati all'applicazione che non dispongono di un criterio assegnato.
  - **SQL Server** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft SQL Server.
  - **Exchange** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft Exchange Server.

  Nota: i gruppi di nodi predefiniti non possono essere modificati o eliminati.
- **Gruppi personalizzati** - Contiene i gruppi di nodi personalizzati.
- **Gruppi vCenter/ESX**: se si aggiunge un nodo all'opzione Importa computer virtuali da vCenter/ESX, il nome del server vCenter/ESX viene aggiunto a tale gruppo.
- **Gruppo Global Dashboard** - Contiene tutti i nodi associati con il server primario centrale.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo per aprire la schermata Nodo.
2. Fare clic su Aggiungi nella barra degli strumenti Gruppo nodi.

   Si aprirà la finestra di dialogo Aggiungi gruppo e verranno visualizzati i nodi nell'elenco Nodi disponibili.
3. Specificare un Nome gruppo per il gruppo di nodi.

4. Completare i seguenti campi della finestra di dialogo Aggiungi gruppo:
   - **Gruppo:**selezionare il nome del gruppo contenente i nodi da assegnare.
   - **Filtro Nome nodo:** consente di filtrare i nodi disponibili in base a un criterio comune.

     Nota: il campo Nome nodo supporta l'uso di caratteri jolly.

     Ad esempio, Acc* consente di filtrare tutti i nodi il cui nome inizia per Acc. Per cancellare i risultati del filtro, fare clic su sul simbolo X del campo Filtro.
5. Per aggiungere nodi al gruppo di nodi, selezionare i nodi che si desidera aggiungere e fare clic sulla freccia destra singola.

   I nodi verranno spostati dall'elenco Nodi disponibili all'elenco Nodi selezionati e assegnati al gruppo di nodi.

   Nota: per selezionare e spostare tutti i nodi dal gruppo corrente, fare clic sulla freccia destra doppia.
6. Se si desidera spostare tutti i nodi dall'elenco Nodi selezionati all'elenco Nodi disponibili fare clic sulla freccia sinistra singola.

   Nota: per selezionare e spostare tutti i nodi dal gruppo corrente, fare clic sulla freccia sinistra doppia.
7. Fare clic su OK.

Il gruppo di nodi verrà aggiunto.

Modifica di gruppi di nodi

L'applicazione consente di modificare i gruppi di nodi creati. È possibile aggiungere o rimuovere i nodi dai gruppi di nodi e modificare il nome dei gruppi.

Nota - I seguenti gruppi di nodi non possono essere modificati:

- **Tutti i nodi** - Contiene tutti i nodi associati con l'applicazione.
- **Nodi senza un gruppo** - Contiene tutti i nodi associati all'applicazione non assegnati a un gruppo di nodi.
- **Nodi senza un criterio** - Contiene tutti i nodi associati all'applicazione che non dispongono di un criterio assegnato.
- **SQL Server** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft SQL Server.
- **Exchange** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft SQL Server.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Fare clic sul gruppo di nodi da modificare, quindi selezionare Modifica nella barra degli strumenti Gruppo nodi.

   Verrà visualizzata la finestra di dialogo Modifica gruppo.

3. Per modificare il nome del gruppo, specificare un nuovo nome nel campo Nome gruppo.

4. Per aggiungere nodi al gruppo nodi, selezionare i nodi che si desidera aggiungere e fare clic sulla freccia destra.

   I nodi verranno spostati dall'elenco Nodi disponibili all'elenco Nodi selezionati e assegnati al gruppo di nodi.

   Nota: per spostare tutti i nodi dall'elenco Nodi disponibili all'elenco Nodi selezionati fare clic sulla freccia destra doppia.

5. Per rimuovere nodi dal gruppo di nodi, fare clic sulla freccia sinistra oppure sulla freccia sinistra doppia per rimuovere rispettivamente uno o tutti i nodi.

6. (Facoltativo) Per filtrare i nodi disponibili in base a criteri comuni, specificare un valore nel Filtro Nome nodo.

   Nota: il campo Filtro supporta l'uso di caratteri jolly.

   Ad esempio, Acc* consente di filtrare tutti i nodi il cui nome inizia per Acc. Per cancellare tutti i risultati del filtro, fare clic sul simbolo X del campo Filtro.

7. Fare clic su OK.

Il gruppo di nodi verrà modificato.

Nota: quando si assegna un nodo Global Dashboard di CA ARCserve Backup a un gruppo nodi, tutti i rami eseguono il rendering sul nodo Global Dashboard di CA ARCserve Backup anche se non tutti rami appartengono allo stesso gruppo di nodi. Pertanto, quando si seleziona il gruppo nodi contenente il nodo Global Dashboard di CA ARCserve Backup nell'applicazione CA ARCserve Central Reporting, i rapporti non conterranno i dati per tutte le diramazioni del nodo Global Dashboard.

Eliminazione di gruppi di nodi

È possibile eliminare un gruppo di nodi in qualsiasi momento. Quando viene eliminato un gruppo aggiunto manualmente, i computer virtuali non vengono rimossi dall'applicazione. Tuttavia, se un gruppo creato automaticamente dal rilevamento di un server ESX o vCenter viene eliminato, il gruppo e tutti i computer virtuali verranno eliminati dall'applicazione.

L'applicazione consente di eliminare i gruppi di nodi creati.

Non è possibile eliminare i seguenti gruppi di nodi:

- **Tutti i nodi** - Contiene tutti i nodi associati con l'applicazione.
- **Nodi senza un gruppo** - Contiene tutti i nodi associati all'applicazione non assegnati a un gruppo di nodi.
- **Nodi senza un criterio** - Contiene tutti i nodi associati all'applicazione che non dispongono di un criterio assegnato.
- **SQL Server** - Contiene tutti i nodi associati con l'applicazione i cui nodi dispongono di Microsoft SQL Server.
- **Exchange** - Contiene tutti i nodi associati con l'applicazione i cui nodi dispongono di Microsoft Exchange Server.

Nota: il processo di eliminazione dei gruppi di nodi non comporta l'eliminazione dei singoli nodi dall'applicazione.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo per aprire la schermata Nodo.

2. Fare clic sul gruppo di nodi da eliminare, quindi su Elimina nella barra degli strumenti Gruppo nodi.

   Verrà visualizzata una finestra di dialogo di conferma.

3. Se si è sicuri di voler eliminare il gruppo dei nodi, fare clic su Sì.

   Nota: fare clic su No se non si desidera cancellare il gruppo di nodi.

Il gruppo dei nodi viene eliminato.

Ricerca di nodi mediante il rilevamento

CA ARCserve Central Protection Manager consente di eseguire la ricerca di nodi utilizzando la funzionalità di rilevamento. Protection Manager esegue la ricerca dei nodi sulla base delle informazioni contenute nel server Active Directory. Active Directory fornisce le seguenti informazioni:

- Nome del computer
- Informazioni sul sistema operativo (nome, versione, patch)
- Installazione di Microsoft Exchange Server sul computer
- Installazione di Microsoft SQL Server sul computer

Per eseguire la ricerca di nodi mediante il rilevamento

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Dalla categoria Nodo, fare clic su Rileva per accedere alla finestra di dialogo Rileva nodi mediante Active Directory.

3. Compilare i seguenti campi finestra di dialogo Rileva nodi mediante Active Directory e fare clic su Aggiungi:

   - (Dominio) Nome utente
   - (Dominio) Password
   - Filtro nome computer

   Fare clic su Rileva.

   Verrà avviato il processo di rilevamento (a pagina 63).

4. Al termine del rilevamento, verrà visualizzato il seguente messaggio di conferma:

   `Continuare ad aggiungere nodi dai risultati di rilevamento?`

   Eseguire una delle seguenti operazioni:

   - Fare clic su Sì per accedere a Aggiungi nodi dai risultati di rilevamento
   - Fare clic su No per chiudere il messaggio.

   Nota: se si seleziona Sì, consultare la sezione Aggiunta di nodi mediante il rilevamento (a pagina 62) per ulteriori informazioni.

Attività di distribuzione di CA ARCserve D2D

CA ARCserve Central Protection Manager consente la distribuzione in locale o in remoto di uno o più nodi contemporaneamente sui sistemi di distribuzione. È inoltre possibile aggiungere o modificare nodi per la distribuzione o eliminarli dalla distribuzione stessa.

In questa sezione verranno presentati i seguenti argomenti:

Distribuzione di CA ARCserve D2D sui nodi

CA ARCserve Central Protection Manager consente di rilevare e distribuire la versione più recente di CA ARCserve D2D a o uno o più nodi nuovi o esistenti.

Nota: per effettuare la distribuzione di CA ARCserve D2D su computer in cui è in esecuzione Windows XP, disattivare l'opzione Utilizza condivisione file semplice del computer remoto Windows XP.

Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.
2. Dalla schermata Nodo, fare clic su Distribuzione dalla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Contratto di licenza.
3. Leggere e accettare i termini del contratto di licenza e fare clic su Avanti per aprire la finestra di dialogo Distribuzione D2D.
4. Dalla finestra di dialogo Distribuzione D2D, specificare il filtro Gruppo e Nome nodo per i nodi disponibili basati su un criterio comune.

   Vengono visualizzati il nome, la versione e lo stato di ciascun nodo.

   Nota: la colonna Versione mostra la versione di D2D corrente eseguita dal nodo.
5. Fare clic sulle caselle di controllo accanto ai nodi corrispondenti, oppure fare clic su Seleziona tutto per eseguire la distribuzione di tutti i nodi elencati per la distribuzione di D2D.

   Nota: quando si fa clic su Seleziona tutto, l'opzione Deseleziona tutto viene attivata automaticamente. Inoltre, se si seleziona un nodo dall'elenco Nodo, è possibile modificare i campi di nodo dalla scheda Informazioni nodo.
6. Fare clic su Distribuisci ora per distribuire la versione più recente di D2D sui nodi (quella visualizzata nella barra del titolo).

   Nota: per visualizzare le informazioni e lo stato di distribuzione di un nodo specifico, evidenziare il nodo e selezionare la scheda corrispondente dal riquadro di destra.

Nota: CA ARCserve Central Protection Manager consente di installare, aggiornare e distribuire l'ultima versione di CA ARCserve D2D a versioni precedenti o nodi mediante l'utilità di distribuzione D2D senza bisogno di installare CA ARCserve D2D.

Aggiunta di nodi per la distribuzione

CA ARCserve Central Protection Manager consente di aggiungere uno o più nodi per la distribuzione.

Per aggiungere nodi per la distribuzione

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.
2. Dalla schermata Nodo, fare clic su Distribuzione dalla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Contratto di licenza.

3. Leggere e accettare i termini del contratto di licenza, quindi fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Distribuzione D2D.

4. Fare clic su Aggiungi e completare i seguenti campi della finestra di dialogo Distribuzione D2D:
   - Nome server
   - Nome utente
   - Password
   - Porta
   - Percorso installazione
   - Consenti al programma di installazione di installare il driver (selezionato per impostazione predefinita)
   - Riavvia (impostazione predefinita: Sì)

     Se la distribuzione del nodo viene completata con il riavvio del sistema (Sì), il nodo viene aggiunto all'elenco nodi gestito da CA ARCserve Central Applications.

     Se la distribuzione del nodo viene completata senza il riavvio del sistema (No), il nodo viene aggiunto all'elenco nodi non gestito da CA ARCserve Central Applications.

   - Usa HTTPS (il valore predefinito è No)

     Il protocollo HTTPS (sicuro) garantisce una maggiore sicurezza delle comunicazioni rispetto al protocollo HTTP. Il protocollo di comunicazione HTTPS è consigliato se si trasmettono informazioni riservate sulla rete.

   Nota: è possibile visualizzare i nodi aggiunti nel filtro Tutti i nodi e Nessun raggruppamento.

5. Fare clic su OK per aggiungere i nodi.

Modificare i nodi per la distribuzione

CA ARCserve Central Protection Manager consente di modificare uno o più nodi per la distribuzione.

Per modificare i nodi per la distribuzione

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.
2. Dalla schermata Nodo, fare clic su Distribuzione dalla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Contratto di licenza.
3. Leggere e accettare i termini del contratto di licenza, quindi fare clic su Avanti.

   Verrà visualizzata la schermata Distribuzione D2D.
4. Selezionare il nodo che si desidera modificare per la distribuzione e fare clic su Modifica per aprire la finestra di dialogo Modifica.
5. Nella finestra di dialogo Modifica, apportare le modifiche desiderate ai dati e fare clic su OK.

Eliminazione di nodi dalla distribuzione

CA ARCserve Central Protection Manager consente di eliminare uno o più nodi dalla distribuzione.

Per eliminare nodi dalla distribuzione

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.
2. Dalla schermata Nodo, fare clic su Distribuzione dalla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Contratto di licenza.
3. Leggere e accettare i termini del contratto di licenza, quindi fare clic su Avanti.

   Verrà visualizzata la schermata Distribuzione D2D.
4. Selezionare i più nodi che si desidera eliminare dalla distribuzione.
5. Fare clic su Elimina per eliminare i nodi dalla distribuzione D2D.

Filtraggio di gruppi di nodi

CA ARCserve Central Protection Manager consente l'utilizzo di filtri per visualizzare i nodi di un gruppo su cui è installata una determinata applicazione. Il filtro è disponibile per le seguenti applicazioni:

- CA ARCserve Backup
- CA ARCserve D2D
- Microsoft SQL Server
- Microsoft Exchange Server

Per filtrare i gruppi di nodi

1. Accedere a CA ARCserve Central Protection Manager.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Nell'elenco Gruppi selezionare il gruppo che si desidera filtrare.

   Nota: è possibile filtrare tutti i gruppi predefiniti (Tutti i nodi, Non assegnato, SQL Server, Exchange) e i gruppi con nome personalizzato.

   Dalla barra degli strumenti Filtro, selezionare la casella di controllo corrispondente all'applicazione che si desidera filtrare.

Il gruppo di nodi viene filtrato.

Modalità di gestione dei criteri CA ARCserve D2D

CA ARCserve Central Protection Manager fornisce diversi strumenti e opzioni per la gestione dei criteri di CA ARCserve D2D. Questa sezione contiene informazioni sull'aggiunta, l'eliminazione, la modifica, la copia e la distribuzione di criteri D2D sui server remoti. È possibile creare criteri di backup centralizzati da distribuire simultaneamente su più nodi gestiti.

Di seguito sono riportati alcuni esempi di criteri di backup centralizzati:

- Pianificazioni
- Processi
- Destinazioni
- Eventi
- Impostazioni

In questa sezione verranno illustrati i seguenti argomenti:

Creazione di criteri

CA ARCserve Central Protection Manager consente di creare uno o più criteri da assegnare ai nodi D2D.

Procedere come descritto di seguito:

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri dalla barra di navigazione per accedere alla schermata Criteri.
2. Fare clic sul pulsante Nuovo per aprire la finestra di dialogo Nuovo criterio.
3. Immettere il nome del criterio e completare i campi obbligatori nelle schede Impostazioni di backup (a pagina 89), Impostazioni di copia file (a pagina 105), Copia punti di ripristino (a pagina 122) e Preferenze. (a pagina 126)
4. Fare clic su Salva.

Il nuovo criterio viene salvato; viene visualizzato un messaggio in cui viene richiesto se si desidera assegnare il criterio ai nodi. Facendo clic su No, viene visualizzato il nuovo criterio nella schermata Criteri. Facendo clic su Sì, viene visualizzata la schermata Assegnazione/Annullamento assegnazione criterio (a pagina 140).

Gestione delle impostazioni di backup

Le impostazioni consentono di specificare il comportamento del backup, quali l'origine e la destinazione di backup, la pianificazione di ciascun tipo di backup e le impostazioni standard e avanzate dei processi di backup. È possibile modificare queste impostazioni in qualsiasi momento, dalla schermata Criteri.

Per gestire le impostazioni di backup, fare clic su Criteri sulla barra di spostamento nella pagina principale e fare clic su Nuovo.

In questa sezione verranno presentati i seguenti argomenti:

Definizione delle impostazioni di protezione

CA ARCserve Central Protection Manager consente di specificare le impostazioni di protezione per i dati di cui si desidera eseguire il backup.

Per specificare le impostazioni di protezione

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la scheda Impostazioni di backup della finestra di dialogo Nuovo criterio, con l'opzione Impostazioni di protezione.

3. Specificare la **destinazione di backup**.

   È possibile specificare un percorso locale (volume o cartella) oppure una cartella condivisa remota (o unità mappata) come posizione di backup.

   a. Se si sceglie di eseguire il backup in un percorso locale (volume o cartella), la destinazione di backup specificata non deve coincidere con il percorso di origine del backup. Nel caso in cui l'origine sia stata inclusa inavvertitamente nella destinazione, tale parte dell'origine verrà esclusa dal backup.

Ad esempio, se si sta tentando di eseguire il backup completo di un computer locale costituito dai volumi C, D ed E, e il volume E viene specificato come destinazione, CA ARCserve D2D esegue solamente il backup dei volumi C e D sul volume E. I dati del volume E non verranno inclusi nel backup. Se si desidera eseguire il backup di tutti i volumi locali, è necessario specificare una posizione remota per la destinazione.

Importante. Verificare che il volume di destinazione specificato non contenga informazioni di sistema, altrimenti il backup non potrà essere eseguito e il sistema non potrà essere recuperato dopo il ripristino bare metal (BMR) in caso di necessità.

Nota: i dischi dinamici non possono essere ripristinati a livello del disco. Se il backup dei dati viene eseguito su un volume che risiede su un disco dinamico, tale disco non potrà essere ripristinato durante il ripristino bare metal.

b. Se si sceglie di eseguire il backup in una posizione condivisa remota, è fondamentale specificare un percorso oppure individuare la posizione desiderata, quindi fornire le credenziali utente (nome utente e password) per accedere al computer remoto.

c. Se la destinazione di backup specificata ha subito modifiche dall'ultimo backup, sarà necessario indicare il tipo di backup. Queste opzioni vengono abilitate quando si modifica la destinazione di backup. Le opzioni disponibili sono Backup completo e Backup incrementale.

- **Backup completo** - Specifica che il backup successivo è un backup completo. La nuova destinazione di backup non dipende dalla destinazione di backup precedente. Se si prosegue con il backup completo, il percorso precedente non viene più richiesto per il completamento dei backup. È possibile conservare il backup precedente allo scopo di eseguire un eventuale ripristino, oppure eliminarlo se non si desidera utilizzarlo a tale scopo. Non viene apportata alcuna modifica ai backup successivi.

- **Backup incrementale** - Specifica che il backup successivo è un backup incrementale. Il processo di backup incrementale successivo verrà eseguito sulla nuova destinazione senza effettuare la copia di tutti i backup dalla destinazione precedente. Tuttavia, la nuova posizione dipende da quella precedente in quanto le modifiche includono solo i dati incrementali (e non i dati del backup completo). Non eliminare i dati dalla posizione precedente. Se la destinazione di backup viene modificata e la destinazione di backup precedente non esiste più, non sarà possibile eseguire il backup incrementale.

4. Specificare l'**origine di backup**.

   È possibile impostare il backup dell'intero computer oppure di un singolo volume del computer.

   - **Backup dell'intero computer** - Specifica l'esecuzione di un backup dell'intero computer. Tutti i volumi presenti sul computer vengono sottoposti a backup.

     Nota: se l'opzione di backup completo del computer è stata selezionata, CA ARCserve D2D rileva automaticamente i volumi/dischi collegati al computer e li include nel backup.

     Ad esempio, se si collega un nuovo disco al computer dopo aver configurato le impostazioni di backup, non sarà necessario modificare tali impostazioni in quanto i dati del nuovo disco verranno protetti automaticamente.

   - **Backup di volumi singoli** - La funzionalità di filtraggio dei volumi consente di specificare l'esecuzione del backup soltanto per i volumi selezionati. Ad ogni modo, se viene specificato un volume inesistente nel server remoto di CA ARCserve D2D, il volume viene ignorato automaticamente durante il backup. Ad esempio, se viene richiesto il backup dei volumi C, D, ed E; e assegnato a un server CA ARCserve D2D che contiene solo i volumi C e D, il criterio viene assegnato ai volumi C e D del server, mentre il volume E viene ignorato con il conseguente salvataggio di un messaggio di avviso nel registro attività.

     Inoltre, per i volumi dell'elenco è disponibile l'opzione Seleziona/deseleziona tutto.

     Nota: se si esegue la selezione di determinati volumi per il backup, verrà eseguito il backup dei soli volumi selezionati.

     I messaggi di notifica vengono visualizzati per le condizioni seguenti:

     - **Connesso al ripristino bare metal** - Se il volume di sistema/avvio non viene selezionato per il backup, verrà visualizzato un messaggio di avviso che notificherà all'utente l'impossibilità di utilizzo del backup per il ripristino bare metal.

5. Specificare le **impostazioni di memorizzazione**.

   È possibile impostare il criterio di memorizzazione in base al numero di punti di ripristino da memorizzare (unione delle sessioni) o al numero di set di ripristino da memorizzare (elimina i set di ripristino e disattiva i backup incrementali infiniti).

   - Punto di ripristino: opzione consigliata. Questa opzione consente di sfruttare completamente le funzionalità di backup incrementale infinito e di ridurre lo spazio di archiviazione utilizzato.
   - Set di ripristino: opzione utilizzata generalmente per ambienti di archiviazione di grandi dimensioni. Selezionare questa opzione per creare e gestire i set di backup e ottenere una gestione più efficace dei tempi di backup, in particolare per la protezione di quantità elevate di dati. È possibile utilizzare questa opzione quando i tempi di backup sono prioritari rispetto ai limiti di spazio.

   Impostazione predefinita: Memorizza i punti di ripristino

   Memorizza i punti di ripristino

   Selezionare questa opzione per specificare il numero di punti di ripristino da memorizzare (immagini di backup complete, incrementali e di verifica).

   - **Specificare il numero di punti di ripristino da memorizzare**

     Quando il limite specificato viene superato, CA ARCserve D2D unisce il primo backup incrementale figlio con il backup padre, creando una nuova immagine di base contenente i blocchi padre e figlio meno recenti. Il processo di unione del backup figlio meno recente con il backup padre viene eseguito per tutti i backup successivi. In questo modo è possibile eseguire un numero di backup incrementali infinito senza modificare il valore di memorizzazione.

     Nota: se la destinazione non dispone di sufficiente spazio libero, è possibile ridurre il numero di punti di ripristino salvati.

     Valore predefinito: 31

     Valore minimo: 1

     Valore massimo: 1344

   - **Esegui il processo di unione** - Selezionare una delle seguenti opzioni per eseguire il processo di unione:

     - **Il prima possibile** - Selezionare l'opzione per eseguire il processo di unione in qualsiasi momento.
     - **Ogni giorno durante l'intervallo di tempo seguente** - Selezionare l'opzione per eseguire il processo di unione in un intervallo di tempo specificato. In caso di esecuzione prolungata del processo di unione, l'impostazione di un intervallo di tempo evita l'esecuzione di numero eccessivo di operazioni di I/O sul server di produzione.

       Nota: durante l'impostazione dell'intervallo di tempo per l'esecuzione del processo di unione, assicurarsi che l'intervallo di tempo specificato consenta il completamento dei processi di backup correlati prima dell'avvio del processo di unione.

Memorizza i set di ripristino

Selezionare questa opzione per specificare il numero di set di ripristino da memorizzare. L'impostazione consente di disattivare in modo permanente un numero infinito di backup incrementali, senza dover unire le sessioni. I set di ripristino consentono di ridurre i tempi di completamento dei processi di unione.

- **Specificare il numero di set di ripristino da memorizzare**

  Selezionare questa opzione per specificare il numero di set di ripristino da memorizzare. Un set di ripristino contiene una serie di backup, a partire da un backup completo seguito da backup incrementali, di verifica o completi.

  Set 1 di esempio:

  - Completo
  - Incrementale
  - Incrementale
  - Verifica
  - Incrementale

  Set 2 di esempio:

  - Completo
  - Incrementale
  - Completo
  - Incrementale

  È necessario un backup completo per avviare un nuovo set di ripristino. Il backup che avvia il set viene convertito automaticamente in un backup completo, anche nel caso in cui non venga configurato o pianificato alcun backup.

  Nota: i set di ripristino incompleti non vengono inclusi nel calcolo del set di ripristino esistente. Un set di ripristino viene considerato completo solo in seguito alla creazione del backup di avvio del set di ripristino successivo.

  Impostazione predefinita: 2

  Valore minimo: 1

  Valore massimo: 100

Nota: se si desidera eliminare un set di ripristino per salvare spazio di archiviazione di backup, ridurre il numero di set di memorizzazione; CA ARCserve D2D procederà all'eliminazione dei set di ripristino meno recenti. Non tentare di eliminare il set di ripristino manualmente.

Esempio 1 - Set di ripristino:

- La data/ora di inizio del backup è 06:00 del 20 agosto 2012.
- Ogni 12 ore viene eseguito un backup incrementale.
- Un nuovo set di ripristino viene avviato con l'ultimo backup del venerdì.
- Si desidera mantenere tre set di ripristino.

In questo esempio, un backup incrementale viene eseguito alle 06:00 e alle 18:00 ogni giorno. Il primo set di ripristino viene creato una volta eseguito il primo backup (deve essere un backup completo). Il primo backup completo viene quindi contrassegnato come backup di avvio del set di ripristino. Quando il backup pianificato alle ore 18:00 del venerdì viene eseguito, diviene un backup completo e il backup viene contrassegnato come backup di avvio del set di ripristino.

Esempio 2 - Set di ripristino:

- Specificare 1 come numero dei set di ripristino da memorizzare.

Nota: CA ARCserve D2D mantiene sempre due set in modo che venga mantenuto un set completo prima di avviare il set di ripristino successivo.

Esempio 3 - Set di ripristino:

- Specificare 2 come numero dei set di ripristino da memorizzare.

Nota: CA ARCserve D2D elimina il primo set di ripristino quando il quarto set di ripristino sta per iniziare. In questo modo, quando il primo backup viene eliminato e il quarto è in fase di avvio, restano disponibili sul disco ancora due set di ripristino (il set di ripristino 2 e 3).

Anche se si sceglie di memorizzare un solo set di ripristino, è necessario disporre di spazio sufficiente per almeno due backup completi.

- **Avvia un nuovo set di ripristino ad ogni:**
  - **Giorno selezionato della settimana** - Specifica il giorno della settimana selezionato per l'avvio di un nuovo set di ripristino.
  - **Giorno selezionato del mese** - Specifica il giorno del mese selezionato per l'avvio di un nuovo set di ripristino. Specificare un numero compreso tra 1 e 30, oppure, nel caso di un mese con 28, 29, 30 o 31 giorni, è possibile specificare l'ultimo giorno del mese come data di creazione del set di ripristino.
- **Avviare un nuovo set di ripristino con:**
  - **Primo backup del giorno selezionato** - Specifica il giorno della settimana selezionato per l'avvio di un nuovo set di ripristino.
  - **Ultimo backup del giorno selezionato** - Indica l'avvio di un nuovo set di ripristino con l'ultimo backup pianificato del giorno specificato. Se per l'avvio del set si seleziona l'ultimo backup e, per qualsiasi motivo, questo non viene eseguito, il set verrà avviato con il successivo backup pianificato, convertito in backup completo. Se il backup successivo eseguito è ad hoc (ad esempio, una situazione di emergenza richiede un backup incrementale rapido), è possibile stabilire se eseguire un backup completo per avviare il set di ripristino o un backup incrementale, in modo tale che il backup successivo avvii il set di ripristino.

    Nota: l'ultimo backup potrebbe non essere l'ultimo backup del giorno se si esegue un backup ad hoc.

6. Definire il tipo di **compressione**.

   Selezionare l'opzione per specificare il tipo di compressione da utilizzare per i backup.

   La compressione riduce l'utilizzo dello spazio su disco ma produce un impatto inverso sulla velocità di backup a causa del maggior utilizzo della CPU.

Di seguito sono riportate le opzioni di compressione disponibili:

- **Nessuna compressione**

  Non verrà eseguita alcuna compressione. L'opzione determina un utilizzo minimo della CPU (velocità massima) e un utilizzo massimo dello spazio su disco per la creazione dell'immagine di backup.

- **Compressione standard**

  Verrà eseguito un certo livello di compressione. Questa opzione fornisce un buon bilanciamento tra l'utilizzo della CPU e dello spazio su disco. Si tratta dell'impostazione predefinita.

- **Compressione massima**

  Verrà eseguita la compressione massima. L'opzione implica un utilizzo massimo di CPU (velocità minima) ma utilizza anche una quantità minore di spazio su disco per l'immagine di backup.

Tenere presenti i seguenti scenari:

- Se l'immagine di backup contiene dati non comprimibili, quali immagini JPG, file ZIP e così via, sarà necessario allocare ulteriore spazio di archiviazione per la gestione di tali dati. Se si specificano opzioni di compressione e l'origine del backup contiene dati che non possono essere compressi, si verificherà un aumento generale dell'utilizzo dello spazio su disco.
- Se si modifica il livello di compressione da nessuna compressione a standard o compressione massima oppure da standard o compressione massima a nessuna compressione, il primo backup eseguito dopo la modifica del livello di compressione sarà un backup completo. Dopo l'esecuzione del primo backup completo, tutti i backup successivi (completo, incrementale o di verifica) verranno eseguiti secondo la pianificazione.
- Se la destinazione non dispone di sufficiente spazio libero, è possibile aumentare il livello di compressione del backup.

7. Definire le impostazioni di **crittografia**.

   a. Selezionare il tipo di algoritmo di crittografia da utilizzare per i backup.

      La crittografia dei dati corrisponde alla conversione di dati in un modulo incomprensibile senza un meccanismo di decifratura. La protezione dei dati di CA ARCserve D2D utilizza algoritmi di crittografia AES (Advanced Encryption Standard) per ottenere la massima protezione e riservatezza dei dati.

Le opzioni di formato disponibili sono Nessuna crittografia, AES-128, AES-192 e AES-256. Per disattivare l'opzione di crittografia, selezionare Nessuna crittografia.

- Il backup completo e i relativi backup incrementali e di verifica devono utilizzare lo stesso algoritmo di crittografia.
- Se l'algoritmo di crittografia viene modificato per il backup incrementale o di verifica, è necessario eseguire il backup completo. In seguito alla modifica dell'algoritmo di crittografia, la prima esecuzione del backup sarà di tipo completo, indipendentemente dal tipo di backup impostato.

  Ad esempio, se si modifica il formato dell'algoritmo e si procede all'invio manuale di un backup incrementale o di verifica personalizzato, il backup si converte automaticamente in backup completo.

b. Nel caso in cui venga selezionato un algoritmo di crittografia, è necessario specificare e confermare una password di crittografia.

- La password di crittografia può contenere un massimo di 23 caratteri.
- Il backup completo e i relativi backup incrementali e di verifica devono utilizzare la stessa password di crittografia.
- Se la password di crittografia di un backup incrementale o di verifica viene modificata, è necessario eseguire il backup completo. In seguito alla modifica della password di crittografia, la prima esecuzione del backup sarà di tipo completo, indipendentemente dal tipo di backup impostato.

  Ad esempio, se si modifica la password di crittografia e si procede all'invio manuale di un backup incrementale o di verifica personalizzato, il backup si converte automaticamente un backup completo.

c. CA ARCserve D2D gestisce le password di crittografia affinché non sia necessario memorizzare tali password.

- La password viene crittografata.
- La password viene memorizzata e non verrà richiesta in caso di ripristino sul computer.
- La password viene richiesta nel caso in cui si desideri eseguire il ripristino su un computer diverso.
- La password viene richiesta nel caso in cui si esegua l'esportazione di un punto di ripristino contenente dati crittografati appartenente ai backup eseguiti sul computer corrente.
- La password viene richiesta se si tenta di ripristinare i dati crittografati da un punto di ripristino esportato.
- La password non viene richiesta per selezionare un punto di ripristino crittografato.
- La password viene richiesta per eseguire il ripristino bare metal.

d. Se è l'opzione di crittografia è abilitata, il registro attività viene aggiornato.

- Viene registrato un messaggio nel registro attività per descrivere l'algoritmo di crittografia selezionato per ciascun backup.
- Viene registrato un messaggio nel registro attività indicante il motivo per cui un backup incrementale o di verifica è stato convertito in un backup completo (modifica della password o dell'algoritmo).

Nota: non è necessario utilizzare le stesse impostazioni di crittografia per tutti i backup. Queste impostazioni possono essere modificate in qualsiasi momento, anche in seguito all'esecuzione di più backup degli stessi dati.

8. Specificare il **limite di velocità del backup**.

   È possibile specificare la velocità massima di scrittura (MB/min) del backup e limitare la velocità di backup per ridurre l'utilizzo della CPU o della rete. Tuttavia, la limitazione della velocità di backup potrebbe influire sul tempo di completamento del processo di backup. Con una velocità di backup inferiore, il tempo di completamento del backup aumenta.

   Nota: per impostazione predefinita, l'opzione Limite di velocità del backup non è attivata e la velocità di backup non viene controllata.

9. Fare clic su Salva.

Le impostazioni di protezione vengono salvate.

Definizione della pianificazione di backup

CA ARCserve Central Protection Manager consente di specificare la pianificazione dei backup.

Per definire la pianificazione di backup

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la finestra di dialogo Nuovo criterio.

3. Fare clic sulla scheda Pianificazione.

   Verrà visualizzata la finestra di dialogo delle opzioni di pianificazione.

4. Specificare le opzioni di pianificazione di backup:

   - **Imposta data e ora di inizio** - Specifica la data e l'ora di inizio dei backup pianificati.

     Nota: durante l'impostazione dell'intervallo di tempo tra i processi di backup ripetuti, assicurarsi che il processo precedente e i processi di unione corrispondenti dispongano del tempo necessario per il loro completamento prima dell'avvio del processo di backup successivo. È possibile calcolare questo valore di tempo in base alla cronologia e all'ambiente di backup in uso.

   - **Backup incrementale** - Specifica la pianificazione dei backup incrementali.

     CA ARCserve D2D esegue il backup incrementale dei blocchi modificati rispetto all'ultimo backup, in base alla pianificazione specificata. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Si tratta della modalità di backup ottimale e si consiglia di utilizzarla come modalità predefinita.

     Le opzioni disponibili sono Ripeti e Mai. Se si seleziona l'opzione Ripeti, è necessario specificare il l'intervallo di tempo (in minuti, ore o giorni) tra i tentativi di backup. L'intervallo minimo per l'esecuzione di un backup incrementale è di 15 minuti.

     Per impostazione predefinita, la pianificazione dei backup incrementali è impostata con cadenza giornaliera.

   - **Backup completo** - Specifica la pianificazione dei backup completi.

     CA ARCserve D2D esegue il backup completo di tutti i blocchi utilizzati sul computer di origine in base alla pianificazione specificata. Le opzioni disponibili sono Ripeti e Mai. Se si seleziona l'opzione Ripeti, è necessario specificare il l'intervallo di tempo (in minuti, ore o giorni) tra i tentativi di backup. L'intervallo minimo per l'esecuzione di un backup completo è di 15 minuti.

     Per impostazione predefinita, la pianificazione per i backup completi è impostata su Mai (nessuna ripetizione pianificata).

   - **Backup di verifica** - Specifica la pianificazione dei backup di verifica.

     In base alla pianificazione specificata, CA ARCserve D2D controlla che i dati protetti siano validi e completi eseguendo una verifica di affidabilità dell'immagine di backup archiviata sull'origine di backup originale. Se necessario esegue la risincronizzazione dell'immagine. Il backup di verifica individua il backup più recente di ciascun blocco e ne confronta le informazioni con l'origine. Questo confronto consente di verificare che le informazioni corrispondenti all'origine siano contenute nel blocco di backup più recente. Se l'immagine di backup di ciascun blocco non corrisponde all'origine (probabilmente a causa di modifiche apportate al sistema dopo l'ultimo backup), CA ARCserve D2D aggiorna (risincronizza) il backup del blocco corrispondente. Sebbene si tratti di una procedura poco frequente, il backup di verifica può essere utilizzato per ottenere le stesse garanzie di un backup completo, senza occupare lo spazio richiesto da questo tipo di backup.

Il backup di verifica presenta il vantaggio di generare immagini di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente. D'altra parte, il backup di verifica richiede tempi di esecuzione più lunghi, in quanto CA ARCserve D2D deve eseguire il confronto di tutti i blocchi di backup originali con i blocchi del backup più recente.

Le opzioni disponibili sono Ripeti e Mai. Se si seleziona l'opzione Ripeti, è necessario specificare il l'intervallo di tempo (in minuti, ore o giorni) tra i tentativi di backup. L'intervallo minimo per l'esecuzione di un backup di verifica è di 15 minuti.

Per impostazione predefinita, la pianificazione per i backup di verifica è impostata su Mai (nessuna ripetizione pianificata).

5. Fare clic su Salva.

Le impostazioni della pianificazione di backup vengono salvate.

Nota: in caso di pianificazione simultanea di più tipi di backup, l'ordine di esecuzione verrà stabilito in base alle seguenti priorità:

- Priorità 1 - Backup completo
- Priorità 2 - Backup di verifica
- Priorità 3 - Backup incrementale

Ad esempio, se è prevista l'esecuzione contemporanea di questi tre tipi di backup, CA ARCserve D2D eseguirà il backup completo. Se non è stato pianificato un backup completo, ma è prevista l'esecuzione simultanea di un backup incrementale e di verifica, CA ARCserve D2D eseguirà il backup di verifica. Il backup incrementale pianificato verrà eseguito solo nel caso in cui non esista alcun conflitto con un altro tipo di backup.

Definizione delle impostazioni avanzate di backup

CA ARCserve Central Protection Manager consente di specificare impostazioni avanzate di backup.

Per definire le impostazioni avanzate di backup

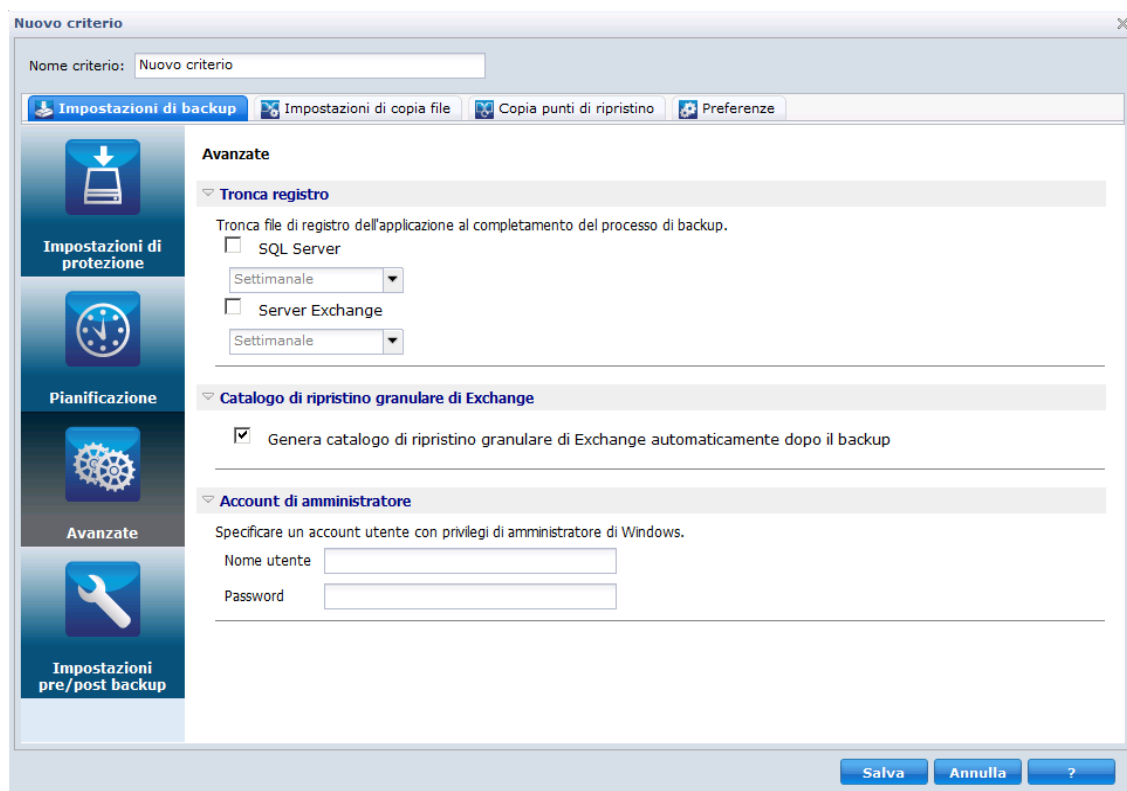
1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la finestra di dialogo Nuovo criterio.

3. Fare clic sulla scheda Avanzate.

   Verrà visualizzata la finestra di dialogo Impostazioni avanzate.

4. Specificare le opzioni di impostazione avanzate.

   - **Tronca registro** - I file di registro delle transazioni accumulate delle applicazioni selezionate vengono troncati in seguito al completamento del backup successivo.

     Il backup eseguito da CA ARCserve D2D è composto da un'immagine snapshot e dai file di registro transazioni creati per tale immagine. Dopo un periodo di tempo, i file di registro transazioni eseguiti non sono più necessari e devono essere eliminati affinché i nuovi file di registro dispongano dello spazio necessario. Il processo di eliminazione dei file di registro viene denominato troncamento del registro. Questa opzione consente di attivare il troncamento dei file di registro delle transazioni, risparmiando spazio su disco.

     Le opzioni disponibili sono SQL Server e Exchange Server. È possibile selezionare una, entrambe o nessuna applicazione. Se viene selezionata una di queste applicazioni, è possibile pianificare un intervallo di tempo (giornaliero, settimanale o mensile) per il troncamento automatico del file di registro:

     Nota: non è possibile troncare i file di registro transazioni se il backup non è stato eseguito correttamente.

     – **Giornaliero** - L'eliminazione dei registri di transazione viene eseguita ogni giorno, dopo il completamento del backup.

     – **Settimanale** - L'eliminazione dei registri di transazione viene eseguita sette giorni dopo il completamento del processo di backup.

     – **Mensile** - L'eliminazione dei registri di transazione viene eseguita trenta giorni dopo il completamento del processo di backup.

     Se un processo di backup è in corso al momento dell'esecuzione pianificata dell'eliminazione, l'operazione di eliminazione viene posticipata al processo pianificato successivo.

     Ad esempio:

     Se un backup incrementale è stato pianificato per essere eseguito ogni giorno alle 17.00 e viene avviato un backup completo alle 16.55, il backup verrà completato alle 17.10.

     In questo caso, il backup incrementale pianificato alle 17.00 viene ignorato, in quanto il backup completo ad hoc è ancora in corso. I file di registro transazione verranno eliminati una volta completato il processo di backup successivo. In questo caso l'eliminazione verrà eseguita il giorno successivo al completamento del backup incrementale pianificato alle ore 17.00.

- **Ripristino granulare di Exchange** - Specifica se abilitare il backup del ripristino granulare di Exchange, per la generazione dei cataloghi di ripristino granulare di Exchange durante ciascun backup.

  Il backup del ripristino granulare di Exchange acquisisce le informazioni relative ai livelli di messaggio, di cartella e della casella di posta elettronica di Exchange in un unico backup del database di Exchange. Attivare questa opzione per eseguire il recupero granulare del database di Exchange selezionando da un elenco gli oggetti Exchange e specificando esattamente i dati che si desidera recuperare senza dover eseguire il recupero o il dump del database di Exchange in un percorso alternativo.

  - Questa opzione consente di creare un catalogo di ripristino granulare di Exchange ed evitare in tal modo i lunghi tempi di esplorazione per il ripristino.
  - Tuttavia, la generazione del catalogo di ripristino granulare di Exchange durante ciascun backup rallenta il completamento del processo di backup e comporta un carico di lavoro superiore. CA ARCserve D2D deve infatti accedere ad ogni casella di posta, eseguire l'autenticazione e generare le informazioni granulari. Questa operazione, in base al numero di caselle di posta e alla dimensione dei dati, può risultare dispendiosa in termini di tempo.
  - Se l'opzione Ripristino granulare di Exchange non viene abilitata, CA ARCserve D2D salva solamente le informazioni di base di Exchange. Prima di eseguire il ripristino, è possibile generare un catalogo Ripristino granulare di Exchange.

- **Account di amministratore** - Specifica il nome utente e la password con i diritti di accesso per l'esecuzione del backup. CA ARCserve D2D verifica la validità del nome utente e della password e che l'utente appartenga a un gruppo amministratori.

  Tenere presenti le seguenti considerazioni:

  - Per specificare un account di dominio, il nome utente del dominio deve essere completo e presentare il formato <nome dominio>\<nome utente>.
  - Se le informazioni dell'account amministratore del server CA ARCserve D2D vengono modificate (nome utente, password), è necessario configurare le informazioni dell'account amministratore in questa finestra di dialogo.
  - Se le credenziali account dell'amministratore non vengono specificate, CA ARCserve D2D immette automaticamente le informazioni relative all'account in cui verrà distribuito il criterio.

5. Fare clic su Salva.

Le impostazioni avanzate di backup vengono salvate.

Definizione delle impostazioni di pre/post backup

CA ARCserve Central Protection Manager consente di specificare le impostazioni di backup.

Per definire le impostazioni pre/post backup

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la finestra di dialogo Nuovo criterio.

3. Fare clic sulla scheda Impostazioni pre/post backup.

   Verrà visualizzata la finestra di dialogo delle opzioni relative alle impostazioni pre/post backup.

4. Specificare le opzioni di impostazione del backup.

   - **Azioni** - Specifica l'esecuzione di comandi script per le azioni da eseguire prima dell'avvio del backup in seguito all'acquisizione dell'immagine snapshot, e/o dopo il completamento del backup. È inoltre possibile attivare i comandi script in base al codice di uscita specifico, quindi selezionare l'azione da eseguire (Esegui processo o Interrompi processo) quando il codice di uscita viene restituito.

     - Se viene selezionata un'azione di tipo Esegui processo, l'esecuzione del processo non viene interrotta se viene restituito il codice di uscita specificato.

     - Se viene selezionata un'azione di tipo Interrompi processo, l'esecuzione del processo viene annullata se viene restituito il codice di uscita specificato.

5. Fare clic su Salva.

Le impostazioni di pre/post backup vengono salvate.

Gestione delle impostazioni di copia di file

Prima di eseguire il primo processo di copia file, è necessario specificare le impostazioni e i criteri di Copia file. Tali configurazioni consentono di specificare determinati comportamenti, quali l'origine dei dati di copia file, la destinazione dei file copiati, la pianificazione di ciascun processo di copia file, nonché le impostazioni e i filtri applicati ai processi di copia file. È possibile modificare queste impostazioni in qualsiasi momento, dalla schermata Criteri.

Definizione dell'origine di copia file

CA ARCserve Central Protection Manager consente di specificare i file di origine che si desidera copiare in una destinazione specifica.

Per definire l'origine di copia file

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la finestra di dialogo Nuovo criterio.

3. Selezionare la scheda Impostazioni di copia file.

   Verrà visualizzata al finestra di dialogo Impostazioni di copia file - Origine.

4. (Facoltativo) Selezionare l'opzione Abilita copia file per convalidare e salvare le modifiche apportate alle impostazioni di copia file. Questa opzione è disattivata per impostazione predefinita.

5. Definire le impostazioni dell'origine di copia file.

   Origini di copia file

   Consente di specificare manualmente le origini di copia, i criteri corrispondenti (filtri) e il tipo di copia file (copia e memorizzazione oppure copia e spostamento) da eseguire in seguito a ciascun backup CA ARCserve D2D completato. È possibile aggiungere, rimuovere o modificare le origini di copia dei file.

   Nota: CA ARCserve D2D non eseguirà la copia dei file di applicazione, dei file con attributi di sistema o dei file con attributi temporanei.

   - **Aggiunta di un'origine**

     Fare clic su questa opzione per visualizzare la finestra di dialogo Tipo di criterio e selezionare il tipo di processo di copia file da eseguire (copia e memorizzazione o copia e spostamento). Dopo aver selezionato il tipo di criterio, viene visualizzata la finestra di dialogo Criterio di copia dei file che consente di aggiungere un'origine da copiare e di specificare i criteri corrispondenti per tale origine. Per ulteriori informazioni, consultare la sezione Definizione dei criteri di copia file (a pagina 108).

     Nota: per il processo di copia file è possibile utilizzare solamente un'origine di cui è stato eseguito il backup. Non è possibile aggiungere un'origine da un volume di cui non è stato eseguito precedentemente il backup con CA ARCserve D2D.

   - **Rimuovi**

     Fare clic su questa opzione per rimuovere l'origine selezionata dall'elenco visualizzato.

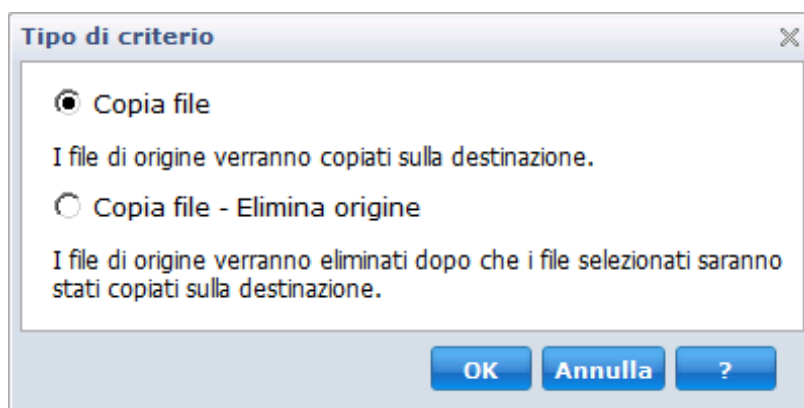
   - **Modificare**

     Fare clic su questa opzione per visualizzare la finestra di dialogo Criteri di copia file e modificare le impostazioni dei criteri per l'origine selezionata. Per ulteriori informazioni, consultare la sezione Definizione dei criteri di copia file (a pagina 108).

6. Fare clic su Salva impostazioni.

Le impostazioni di copia file vengono salvate.

Definizione dei criteri di copia dei file

Fare clic sull'opzione per l'aggiunta di un'origine di Copia file per visualizzare la finestra di dialogo Tipo di criterio e selezionare il tipo di processo di copia file da eseguire.

I tipi di criterio disponibili sono Copia file e Copia file - Elimina origine.

Copia file

I dati vengono copiati dal sistema di origine al sistema di destinazione (vengono conservati nella posizione di origine). Sono disponibili più versioni archiviate.

Copia file - Elimina origine

I dati vengono trasferiti dal sistema di origine al sistema di destinazione (ed eliminati dal percorso di origine) liberando spazio sull'origine.

Se si seleziona Copia file - Elimina origine, viene visualizzato un messaggio di avviso per informare l'utente che i dati di copia file verranno eliminati e non saranno più disponibili nella posizione originale. Fare clic su OK per visualizzare la finestra di dialogo Criteri di copia file.

Importante: Per i file copiati utilizzando l'opzione Copia file - Elimina origine, CA ARCserve D2D genera un file stub con estensione D2DARC. Il file stub contiene informazioni sulla destinazione e la data di spostamento dei file.

Quando viene specificato il tipo di criterio per l'eliminazione dei dati di cui è stato eseguito il backup, è necessario specificare alcuni criteri correlati. Nella finestra di dialogo Impostazioni di copia file, è possibile aggiungere una nuova origine di copia file oppure modificare un'origine di copia file esistente specificando i criteri nella finestra di dialogo Criteri di copia file.

A seconda del tipo di criterio selezionato, viene visualizzata la finestra di dialogo Criteri di copia file corrispondente; tuttavia le opzioni contenute in ciascuna finestra sono simili.

Opzione selezionata: Copia file

Opzione selezionata: Copia file - Elimina origine

Copia file - Elimina origine

Consente di specificare l'origine di copia file e impostare i criteri corrispondenti, nonché il tipo di copia file da eseguire. È possibile selezionare la posizione di origine.

Filtri di origine

I filtri consentono di limitare il numero di oggetti di copia file ai tipi e valori specificati.

Tipo di filtro

Esistono due tipi di filtri: Includi ed Escludi.

Il filtro Includi esegue la copia file solo degli oggetti dell'origine copia file corrispondenti al valore specificato.

Il filtro Escludi esegue la copia file solo degli oggetti dell'origine copia file corrispondenti al valore specificato.

È possibile specificare più filtri all'interno della stessa copia file separando ciascun valore di filtro con una virgola.

- Se si specificano più filtri di inclusione, i dati che corrispondono ad almeno uno dei filtri verranno inclusi nella copia file.
- Se si specificano più filtri di esclusione, i dati che corrispondono ad almeno uno dei filtri verranno esclusi dalla copia file.
- È possibile combinare i filtri di inclusione ed esclusione nella stessa richiesta di copia file.

Nota: se si verifica un conflitto tra i parametri specificati per i filtri Includi-Escludi, il filtro Escludi viene applicato in quanto è considerato prioritario. Un filtro di inclusione non può eseguire la copia file di un oggetto contrassegnato dal filtro Escludi.

Variabile di filtro (criterio)

Esistono due tipi di filtri a criterio variabile: Criterio file e Criterio cartella.

È possibile utilizzare il filtro Criterio file o Criterio cartella per includere o escludere determinati oggetti dalla copia file.

Valore di filtro

Il valore di filtro consente di limitare le informazioni di copia file selezionando solamente le informazioni di parametro specificate, ad esempio file txt.

CA ARCserve D2D consente di utilizzare caratteri jolly per selezionare più oggetti da includere nella richiesta di copia file. Un carattere jolly è un carattere speciale che può essere utilizzato per rappresentare un carattere singolo o una stringa di testo.

Il campo Valore supporta i caratteri asterisco e punto di domanda. Se non si è a conoscenza del valore completo del criterio file/cartella, è possibile semplificare i risultati del filtro specificando un carattere jolly.

- "*": utilizzare l'asterisco per sostituire uno, nessuno o più caratteri del valore.
- "?": utilizzare il punto interrogativo per sostituire un carattere del valore.

Ad esempio, immettere * .txt per escludere tutti i file con estensione .txt, nel caso in cui non si conosca il nome di un file specifico. È possibile specificare il nome parzialmente ed utilizzare i caratteri jolly per completare le parti mancanti.

Nota: se si seleziona Criterio file come tipo di filtro, viene visualizzato un elenco a discesa contenente filtri predefiniti per i tipi di file più utilizzati (file MS-Office, file Image, file eseguibili, file temporanei, ecc.).

Filtro dimensione file (solo processi Copia file - Elimina origine)

Questo filtro viene applicato solo ai processi Copia file - Elimina origine e non ai processi Copia file.

I filtri di dimensione file consentono di limitare gli oggetti di origine per la copia file in base alla dimensione del file. Se il filtro di dimensione file è attivato, i parametri specificati costituiscono il filtro che definisce gli oggetti da includere nella copia file. È possibile selezionare l'intervallo (Uguale a o Maggiore di, Uguale a o Minore di oppure Tra) e immettere un valore per la dimensione.

Ad esempio, se viene specificato l'intervallo Uguale a o Maggiore di 10MB, CA ARCserve D2D eseguirà la copia file dei soli oggetti che soddisfano questo criterio. Per gli oggetti che non soddisfano i criteri di dimensione dei file non verrà eseguita la copia file.

Filtro data file (solo processi Copia file - Elimina origine)

Questo filtro viene applicato solo ai processi Copia file - Elimina origine e non ai processi Copia file.

I filtri di data file consentono di includere automaticamente gli oggetti di origine per la copia file, in base alle date specificate per il file. È possibile selezionare un parametro (Nessun accesso al file per, File non modificati in, e/o File non creati in) e immettere un valore per il numero di giorni, mesi o anni per il Filtro data file. È possibile selezionare più filtri data file per la copia file automatica.

Ad esempio, se si specifica il parametro File non modificati per 180 giorni, CA ARCserve D2D eseguirà automaticamente la copia file di tutti i file che soddisfano questo criterio, ovvero i file a cui non sono state apportate modifiche durante gli ultimi 180 giorni.

Importante: Se si specificano entrambi i filtri Dimensione file e Data file o più filtri Data file, verrà eseguita la copia file dei soli file che soddisfano tutti i parametri di filtro specificati. I file che non soddisfano nessun parametro non verranno inclusi nella copia file.

Definizione delle destinazioni di copia dei file

CA ARCserve Central Protection Manager consente di specificare le impostazioni di destinazione per le informazioni di cui si desidera eseguire la copia file.

Per definire le destinazioni di copia file

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la finestra di dialogo Nuovo criterio.

3. Selezionare la scheda Impostazioni di copia file, quindi selezionare Destinazione per aprire la finestra di dialogo Destinazione delle Impostazioni di copia file.

4. Specificare le impostazioni di destinazione.

   - **Destinazione** - Consente di specificare il percorso di destinazione per il processo di copia file. È possibile selezionare una sola destinazione.

     CA ARCserve D2D consente di specificare le impostazioni di copia file su un disco o in ambiente cloud per i file di cui è stato eseguito il backup. In caso di copia file, è possibile scegliere di copiare e memorizzare oppure di copiare e spostare i dati di backup. Sebbene i due processi siano simili, se si sceglie di copiare e spostare i dati, questi vengono spostati dal sistema di origine a quello di destinazione ed eliminati dal percorso di origine, aumentando così lo spazio libero sull'origine. Se si sceglie di copiare e memorizzare i dati, questi vengono copiati dal sistema di origine a quello di destinazione e conservati nella destinazione di origine. In questo modo saranno disponibili più versioni archiviate.

     - **Copia file su unità di rete o locale** - Se selezionata, questa opzione consente di specificare il percorso completo della posizione in cui si desidera spostare o copiare i file o le cartelle di origine. È possibile cercare la posizione di destinazione. Fare clic sulla freccia verde per convalidare la connessione alla destinazione specificata.

     - **Copia file su cloud** - Se selezionata, questa opzione consente di specificare la posizione cloud in cui si desidera spostare o copiare i file o le cartelle di origine. Attualmente, CA ARCserve D2D supporta la copia file su più fornitori cloud, quali Amazon S3 (Simple Storage Service), Windows Azure, Fujitsu Cloud (Windows Azure) ed Eucalyptus-Walrus. Tali fornitori cloud corrispondono a servizi Web pubblici che consentono di archiviare e recuperare in modo del tutto sicuro i dati di grandi e piccole dimensioni dal Web, in qualsiasi momento.

       Fare clic sul pulsante Configura per visualizzare la finestra di dialogo Configurazione cloud. Per ulteriori informazioni, consultare la sezione Definizione della configurazione cloud per la copia file (a pagina 117).

       Nota: per eliminare eventuali errori di sfasamento orario durante la connessione all'ambiente cloud, verificare sul computer in uso che il fuso orario sia stato impostato correttamente e che l'orologio sia sincronizzato con l'orario globale. Si consiglia di confrontare l'ora del computer con l'ora GMT. Se l'orario del computer in uso non è sincronizzato con l'ora globale corretta (con uno scarto di 5-10 minuti), non sarà possibile utilizzare Amazon S3. Se necessario, reimpostare l'ora corretta per il computer ed eseguire di nuovo il processo di archiviazione.

     Per entrambe le opzioni di destinazione, se la connessione alla destinazione specificata viene persa o interrotta, CA ARCserve D2D eseguirà più tentativi di completamento del processo di copia file. Nel caso in cui non sia possibile completare il processo, viene eseguito un processo di riparazione a partire dal punto in cui si è verificato l'errore. Inoltre, il registro attività viene aggiornato con il messaggio di errore corrispondente e viene inviata una notifica di posta elettronica (se configurata).

- **Compressione** - Specifica il tipo di compressione da utilizzare per i processi di copia file.

  Generalmente, la compressione viene utilizzata per ridurre lo spazio di archiviazione, tuttavia comporta la riduzione della velocità di copia file a causa del maggiore utilizzo della CPU.

  Le opzioni disponibili sono:

  - **Nessuna compressione** - Non viene eseguito alcun tipo di compressione. L'opzione determina un utilizzo minimo della CPU (velocità massima) e un utilizzo massimo dello spazio di archiviazione per la copia file.
  - **Compressione standard** - Comporta un livello medio di compressione. L'opzione determina un equilibrio di utilizzo della CPU e dello spazio di archiviazione richiesto. Si tratta dell'impostazione predefinita.
  - **Compressione massima** - Verrà applicata la massima compressione. L'opzione determina un utilizzo massimo della CPU (velocità minima) e un utilizzo minimo dello spazio di archiviazione per la copia file.

- **Crittografia** - Consente di abilitare la password di crittografia per la copia di file.
- **Periodo di memorizzazione** - Questa impostazione viene applicata solo ai dati di copia file spostati e non ai dati copiati e memorizzati.

  Specifica la durata (anni, mesi, settimane, giorni) di memorizzazione dei dati archiviati nel percorso di destinazione. Al termine del periodo di memorizzazione specificato, i dati archiviati verranno eliminati dalla destinazione.

  Il calcolo del periodo di memorizzazione si basa sul periodo di un mese di 30 giorni e di un anno di 365 giorni. Ad esempio: Se si specifica un periodo di memorizzazione di 2 anni, 2 mesi e 5 giorni, il tempo di memorizzazione totale per i dati di copia file sarà di 795 giorni (365 + 365 + 30 + 30 + 5).

  Importante. Poiché questa impostazione si applica solo ai dati copiati e spostati dal sistema di origine a quello di destinazione (e non ai dati copiati e memorizzati), alla fine del periodo di memorizzazione specificato i dati vengono eliminati dalla destinazione. Tali dati non verranno né archiviati né salvati.

- **Versioni del file** - Questa impostazione si applica solo ai dati copiati e memorizzati (e non ai dati copiati e spostati).

  Specifica il numero di copie memorizzate e archiviate nel percorso di destinazione (cloud o disco). Quando questo numero viene raggiunto, la versione meno recente viene eliminata. Il processo di eliminazione della versione archiviata meno recente viene ripetuto con l'aggiunta delle nuove versioni alla destinazione mantenendo in questo modo il numero di versioni archiviate specificato.

  Ad esempio, se il valore delle versioni di file da memorizzare viene impostato su cinque e vengono eseguite cinque copie del file alle ore t1, t2, t3, t4 e t5, tali versioni costituiscono le cinque copie di file memorizzate e disponibili per il recupero. Quando viene eseguita la sesta copia (con il salvataggio della nuova versione), CA ARCserve D2D rimuove la copia t1 e le cinque versioni disponibili per il recupero saranno t2, t3, t4, t5 e t6.

  Per impostazione predefinita, il numero di copie memorizzate nel percorso di destinazione è 15.

5. Fare clic su Salva impostazioni.

Le impostazioni di destinazione di copia file vengono salvate.

Definizione dei dettagli della configurazione cloud per la copia file

Il menu a discesa contenuto in questa finestra di dialogo consente di selezionare il tipo di fornitore cloud da utilizzare per l'archiviazione delle copie file. Le opzioni disponibili sono Amazon S3, Windows Azure, Fujitsu Cloud (Windows Azure) e Eucalyptus-Walrus. Il fornitore selezionato per impostazione predefinita è Amazon S3. Per ulteriori informazioni su Fujitsu Cloud (Windows Azure), consultare le sezioni Panoramica e Registrazione.

Nota: se si utilizza Eucalyptus-Walrus come fornitore cloud di copia dei file, non sarà possibile copiare file il cui percorso supera i 170 caratteri.

Le opzioni di configurazione disponibili per ciascun fornitore cloud sono simili (con alcune differenze terminologiche). In caso di differenze viene fornita una descrizione.

1. Specificare le impostazioni di connessione:

   URL del fornitore

   Specifica l'indirizzo URL del provider cloud.

   Per Amazon S3, Windows Azure, e Fujitsu Cloud (Windows Azure), l'URL del fornitore viene compilato automaticamente. Per Eucalyptus-Walrus, è invece necessario immettere manualmente l'URL del fornitore, nel formato specificato.

ID del codice di accesso/Nome account/ID query

Indica l'utente che richiede l'accesso a questa posizione.

Per questo campo, Amazon S3 utilizza ID del codice di accesso, Windows Azure e Fujitsu Cloud (Windows Azure) utilizzano Nome account, e Eucalyptus-Walrus utilizza ID query.

Codice di accesso segreto/Chiave privata

Poiché il codice di accesso non viene crittografato, la chiave privata si utilizza per verificare l'autenticità della richiesta di accesso.

Importante. Il codice di accesso segreto è fondamentale per la protezione dell'account. Si consiglia di archiviare i codici e le credenziali account in una posizione protetta. Non immettere il codice di accesso segreto in pagine Web o in altri codici sorgente accessibili pubblicamente né in comunicazioni su canali non protetti.

Per questo campo, Amazon S3 utilizza Codice di accesso segreto. Windows Azure, Fujitsu Cloud (Windows Azure) e Eucalyptus-Walrus utilizzano il campo Chiave privata.

Abilita proxy

Se si seleziona questa opzione, è necessario includere anche l'indirizzo IP (o il nome del computer) del server proxy e il numero di porta corrispondente utilizzati dal server proxy per la connessione a Internet. Inoltre è possibile selezionare questa opzione se si desidera richiedere l'autenticazione per il server proxy. Sarà quindi necessario fornire le informazioni di autenticazione (nome utente e password) richieste per utilizzare il server proxy.

(La funzionalità di proxy non è disponibile per Eucalyptus-Walrus).

2. Definizione delle impostazioni avanzate:

   Nome bucket/Contenitore

   Tutti i file e le cartelle spostati o copiati sul sistema del fornitore cloud vengono archiviati e organizzati in bucket o contenitori. I bucket sono dei contenitori di file utilizzati per raggruppare e organizzare gli oggetti. Tutti gli oggetti archiviati sul sistema del fornitore cloud vengono inclusi in un bucket.

   Per questo campo, Amazon S3 e Eucalyptus-Walrus utilizzano Nome bucket. Windows Azure e Fujitsu Cloud (Windows Azure) utilizzano Contenitore.

   Nota: a partire da questo punto del passaggio, è possibile applicare le operazioni relative ai bucket ai contenitori, salvo diversamente specificato.

   Per specificare un nuovo nome bucket:

   a. Specificare il nuovo nome bucket.

Nota: CA ARCserve Central Protection Manager non crea il nome del bucket. Tuttavia, viene generato per ciascun nodo CA ARCserve D2D quando avviene l'assegnazione di un criterio CA ARCserve Central Protection Manager. Il nome del bucket di ogni nodo CA ARCserve D2D viene completato con il prefisso "d2dfilecopy-<nome host>-<nome impostato dall'utente>".

Il nome del bucket deve essere univoco, facilmente identificabile e conforme alle regole di denominazione dei domini Internet. Ciascun bucket deve disporre di un nome univoco. La comprensione della sintassi valida per la denominazione dei bucket è fondamentale.

Per ulteriori informazioni sui requisiti di denominazione bucket in Amazon S3 e Eucalyptus-Walrus, consultare la documentazione di Amazon S3.

Per ulteriori informazioni sui requisiti di denominazione dei contenitori Windows Azure e Fujitsu Cloud (Windows Azure), consultare la documentazione di Microsoft.

b. Per Amazon S3, selezionare un'area disponibile dal menu a discesa. Per impostazione predefinita, tutte le aree disponibili vengono incluse nel menu a discesa. È possibile selezionare l'area in cui si desidera inserire il nuovo bucket creato.

   Le aree consentono di selezionare la regione geografica in cui Amazon S3 eseguirà l'archiviazione dei bucket creati. Selezionare un'area che consenta di accedere rapidamente ai dati e ottimizzare la latenza, ridurre i costi, o soddisfare i requisiti normativi.

   Per Windows Azure, Fujitsu Cloud (Windows Azure) e Eucalyptus-Walrus, non è possibile selezionare la regione.

c. Dopo aver specificato i valori, fare clic su OK. Il nome bucket viene convalidato e creato nell'ambiente cloud.

d. Una volta completata la creazione del nuovo bucket, viene visualizzata la finestra di dialogo Configurazione cloud, contenente le informazioni relative al nuovo bucket (nome e area) nei campi delle impostazioni avanzate.

Abilita riduzione di archiviazione dei dati ridondanti

Con Amazon S3, è possibile selezionare questa opzione per abilitare la riduzione di archiviazione dei dati ridondanti (RRS). L'opzione di archiviazione RSS di Amazon S3 consente di ridurre i costi mediante l'archiviazione dei dati non critici e riproducibili a livelli di ridondanza inferiori rispetto ai livelli di archiviazione standard di Amazon S3. Entrambe le opzioni di archiviazione (con ridondanza standard e ridotta) consentono di archiviare i dati su più dispositivi e periferiche. Tuttavia la riduzione di archiviazione dei dati ridondanti consente di eseguire un numero minore di repliche, riducendo in tal modo i costi. L'archiviazione standard di Amazon S3 e la riduzione di archiviazione dei dati ridondanti presentano gli stessi valori di latenza e velocità. Per impostazione predefinita questa opzione non è selezionata, in quanto Amazon S3 utilizza l'opzione di archiviazione standard.

3. Per verificare la connessione al percorso cloud specificato, fare clic su Verifica connessione.
4. Fare clic su OK per uscire dalla finestra di dialogo Configurazione cloud.

Definizione della pianificazione di copia file

CA ARCserve Central Protection Manager consente di specificare le impostazioni di pianificazione delle informazioni di cui si desidera eseguire la copia file.

Per definire la pianificazione di copia file

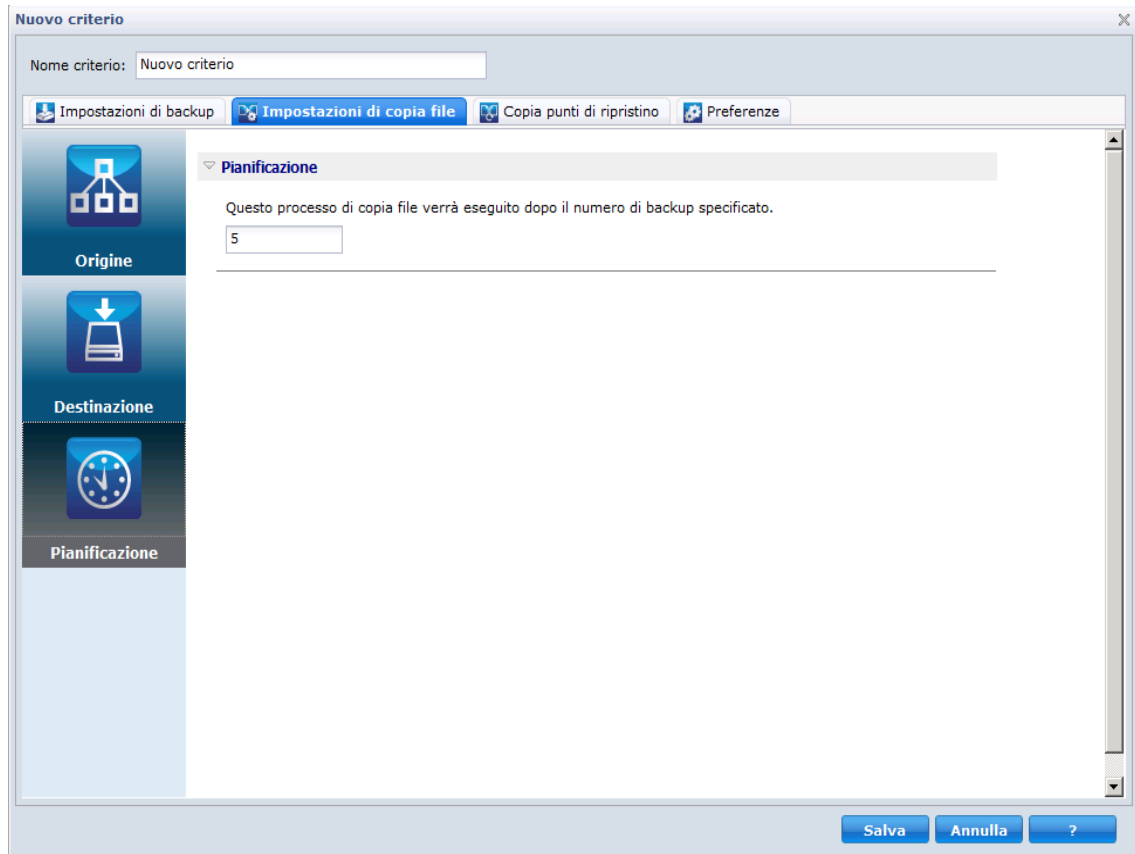
1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la finestra di dialogo Nuovo criterio.

3. Selezionare la scheda Impostazioni di copia file e selezionare Pianificazione.

   Verrà visualizzata al finestra di dialogo Pianificazione delle impostazioni di copia file.

4. Specificare le impostazioni di pianificazione di copia file.

   - **Pianificazione** - Consente di eseguire la copia file dei dati in seguito a un numero determinato di backup.

     Il processo di copia file viene avviato automaticamente dopo l'esecuzione di un numero di backup specificato e sarà basato sui criteri di Copia file selezionati.

     È possibile utilizzare questa impostazione per controllare il numero di attivazioni giornaliere di un processo di copia file. Ad esempio, se si imposta l'esecuzione di un processo di backup ogni 15 minuti, e si specifica l'esecuzione di un processo di copia file ogni 4 backup, verranno eseguite 24 archiviazioni di copia file al giorno (1 ogni ora).

     Per impostazione predefinita, la pianificazione della copia file viene eseguita dopo il completamento di 5 processi di backup. È possibile specificare un numero massimo di 700 backup).

5. Fare clic su Salva impostazioni.

Le impostazioni di pianificazione di copia file vengono salvate.

Definizione delle impostazioni di copia dei punti di ripristino

CA ARCserve D2D consente di specificare le impostazioni di pianificazione della copia e, se necessario, dell'esportazione dei punti di ripristino. Per una migliore comprensione delle modalità di configurazione della pianificazione della copia del punto di ripristino mediante le opzioni disponibili in questa finestra di dialogo, consultare la sezione Copia punti di ripristino - Scenari di esempio.

Nota: il processo di copia del punto di ripristino corrisponde soltanto a un'operazione copia incolla e non a un'operazione taglia incolla. Di conseguenza, ad ogni esecuzione di un processo di copia di un punto di ripristino pianificato, CA ARCserve D2D crea una copia aggiuntiva del punto di ripristino nella destinazione di copia specificata. Allo stesso tempo, mantiene la copia originale del punto di ripristino nella destinazione di backup specificata nelle Impostazioni di backup.

Per definire le impostazioni di copia dei punti di ripristino

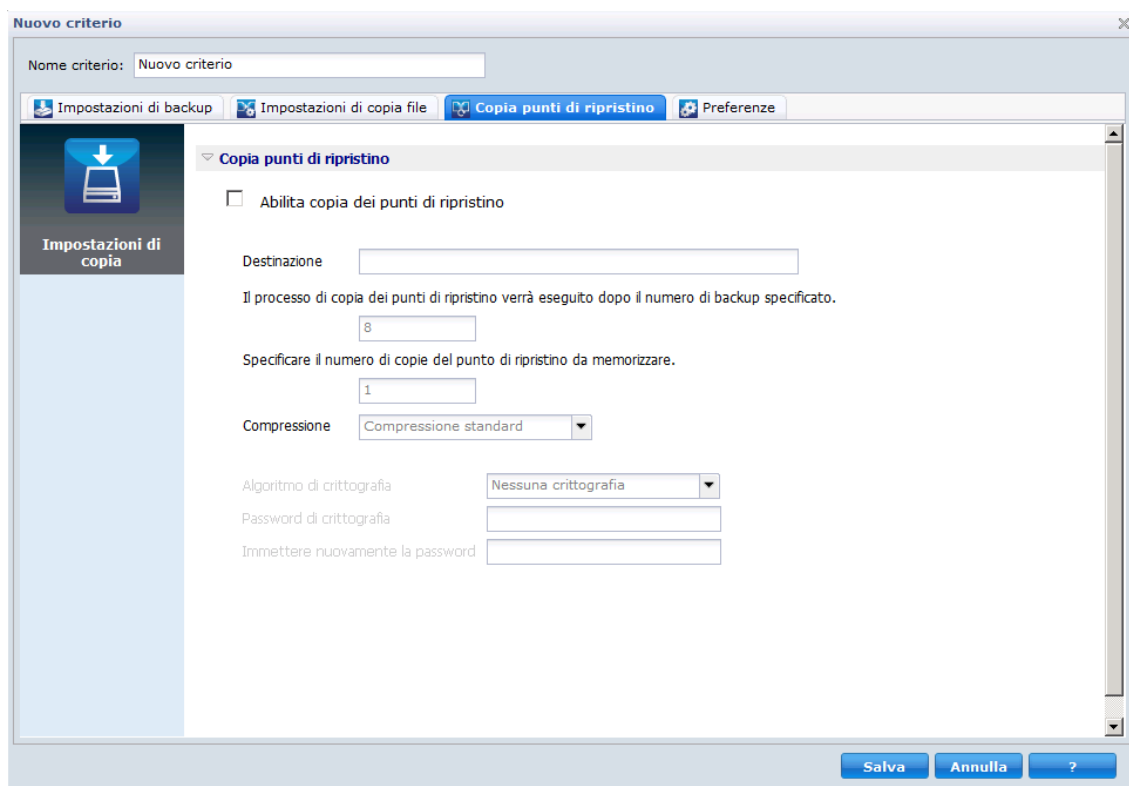
1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la finestra di dialogo Nuovo criterio.

3. Selezionare la scheda Copia punti di ripristino.

   Viene visualizzata la finestra di dialogo Copia punti di ripristino.

4. Specificare le impostazioni di pianificazione della copia del punto di ripristino.

   Abilita copia dei punti di ripristino

   Consente di pianificare la copia dei punti di ripristino in seguito al completamento del numero di backup specificato. Se questa opzione non viene selezionata, non verrà eseguita la copia dei punti di ripristino pianificata.

   Destinazione

   Consente di specificare la posizione (destinazione) della copia dei punti di ripristino oppure di selezionare una posizione di copia. Per verificare la connessione al percorso specificato, fare clic sulla freccia verde.

Il processo Copia punti di ripristino verrà eseguito al completamento del numero di backup specificato.

Consente di specificare quando eseguire l'avvio automatico del processo di copia del punto di ripristino pianificato.

Il processo di copia dei punti di ripristino viene avviato automaticamente dopo l'esecuzione di un numero di backup specificato e viene basato sui criteri di copia selezionati.

È possibile utilizzare questa impostazione per controllare il numero di attivazioni giornaliere di un processo di copia del punto di ripristino. Ad esempio, se si specifica l'esecuzione del processo di backup ogni 15 minuti, e si specifica l'esecuzione della copia dei punti di ripristino in seguito al completamento di 4 backup, verranno eseguiti 24 processi di copia del punto di ripristino al giorno (1 ogni ora).

Per impostazione predefinita, la pianificazione della copia dei punti di ripristino viene eseguita in seguito al completamento di 8 processi di backup.

Importante: Se si pianifica l'esecuzione dei processi backup e di copia a intervalli regolari e il processo di copia è attualmente in esecuzione (stato attivo), non sarà possibile completare l'esecuzione pianificata del processo di backup. Il processo di backup successivo verrà eseguito in base alla pianificazione e verrà completato correttamente solo nel caso in cui non si verifichi un conflitto con un altro processo di copia. Poiché le operazioni di copia e di backup completo richiedono un tempo di esecuzione simile, si consiglia di non impostare una pianificazione frequente dei processi di copia del punto di ripristino.

Specificare il numero di copie di punti di ripristino da memorizzare.

Specifica il numero di punti di ripristino memorizzati e archiviati nella destinazione di copia specificata. Quando questo numero viene raggiunto, la versione meno recente del punto di ripristino viene eliminata. Il processo di eliminazione dei punti di ripristino meno recenti viene ripetuto con l'aggiunta delle nuove versioni alla destinazione mantenendo in questo modo il numero di punti di ripristino archiviati specificato.

Nota: se la destinazione non dispone di sufficiente spazio libero, è possibile ridurre il numero di punti di ripristino salvati.

Per impostazione predefinita, il valore di memorizzazione è impostato su 31 punti di ripristino.

Nota: il numero massimo di punti di ripristino è 1344.

Compressione

Specifica il tipo di compressione da utilizzare per la copia dei punti di ripristino.

La compressione consente solitamente di ridurre l'utilizzo dello spazio su disco. Tuttavia, può avere un effetto inverso e ridurre la velocità di backup a causa dell'aumento dell'utilizzo della CPU.

Le opzioni disponibili sono:

- **Nessuna compressione** - Non viene eseguito alcun tipo di compressione. I file sono di tipo VHD. L'opzione determina un utilizzo minimo della CPU (velocità massima) e un utilizzo massimo dello spazio su disco per la creazione dell'immagine di backup.
- **Nessuna compressione - VHD** - Non viene eseguito alcun tipo di compressione. I file verranno convertiti direttamente in .vhd senza dover ricorrere ad operazioni manuali. L'opzione determina un utilizzo minimo della CPU (velocità massima) e un utilizzo massimo dello spazio su disco per la creazione dell'immagine di backup.
- **Compressione standard** - Comporta un livello medio di compressione. Questa opzione fornisce un buon bilanciamento tra l'utilizzo della CPU e dello spazio su disco. Si tratta dell'impostazione predefinita.
- **Compressione massima** - Verrà applicata la massima compressione. L'opzione implica un utilizzo massimo di CPU (velocità minima) ma utilizza anche una quantità minore di spazio su disco per l'immagine di backup.

Nota: se l'immagine di backup contiene dati non comprimibili (come ad esempio immagini JPG, file ZIP, ecc.), potrebbe essere necessario allocare ulteriore spazio per la gestione di tali dati. Di conseguenza, se si seleziona una qualsiasi opzione di compressione e il backup contiene dati non comprimibili, l'utilizzo di spazio su disco potrebbe aumentare.

Algoritmo di crittografia

Specifica il tipo di algoritmo di crittografia da utilizzare per le copie del punto di ripristino.

La crittografia dati è la conversione dei dati in un formato incomprensibile senza un meccanismo di decifrazione. La protezione dei dati di CA ARCserve D2D utilizza algoritmi di crittografia AES (Advanced Encryption Standard) per ottenere la massima protezione e riservatezza dei dati.

Le opzioni di formato disponibili sono Nessuna crittografia, AES-128, AES-192 e AES-256. Per disattivare l'opzione di crittografia, selezionare Nessuna crittografia.

Password di crittografia

Se il punto di ripristino da copiare è stato crittografato, è necessario immettere e confermare la password.

- Se il punto di ripristino viene copiato in un percorso dello stesso computer, la password di crittografia viene memorizzata e il campo viene compilato automaticamente.
- Se il punto di ripristino è stato copiato su un computer diverso, sarà necessario immettere la password di crittografia.

5. Fare clic su Salva impostazioni.

Le impostazioni di copia del punto di ripristino vengono salvate.

Gestione delle preferenze

CA ARCserve Central Protection Manager consente di gestire le esigenze generali di un criterio. È possibile generare newsfeed o creare notifiche di avviso di posta elettronica oppure, ancora, aggiornare i server e le connessioni.

In questa sezione verranno illustrati i seguenti argomenti:

Definizione delle preferenze della scheda Generale

CA ARCserve Central Protection Manager consente di specificare le preferenze generali di un criterio.

Per definire le preferenze generiche

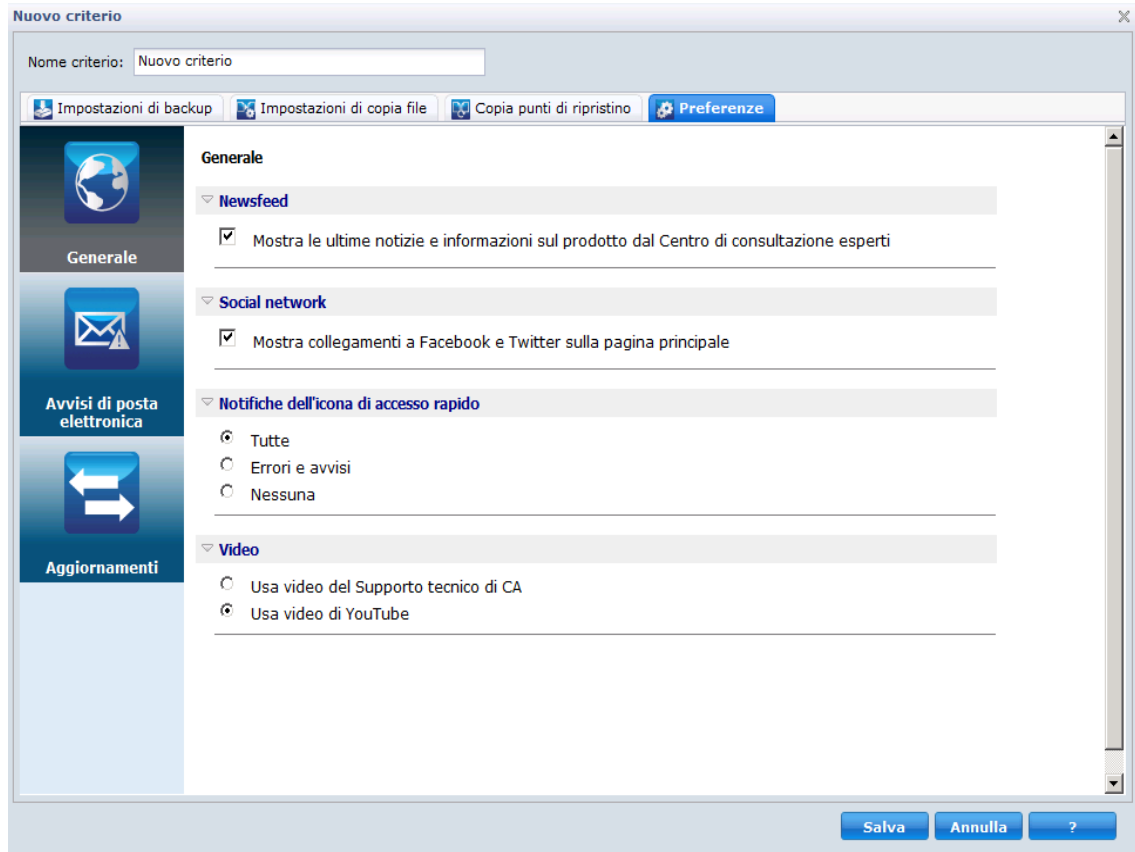
1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la finestra di dialogo Nuovo criterio.

3. Selezionare la scheda Preferenze.

   Verrà visualizzata la finestra di dialogo Preferenze - Generale.

4. Specificare le preferenze

   - **Newsfeed** - Abilitare questa opzione per visualizzare le ultime notizie e informazioni sul prodotto dal Centro di consultazione esperti.
   - **Social network** - Abilitare questa opzione per visualizzare i collegamenti a Facebook e Twitter dalla pagina principale.
   - **Notifiche della barra delle applicazioni** - È possibile selezionare una delle seguenti opzioni:
     - Selezionare Tutto per visualizzare tutte le notifiche sulla barra delle applicazioni.
     - Selezionare Errori e Avvisi per visualizzare solo gli errori e gli avvisi sulla barra delle applicazioni.
     - Selezionare Nessuno se non si desidera visualizzare alcun tipo di notifica.
   - **Video** - Selezionare il tipo di video da utilizzare nel criterio D2D:
     - Video del Supporto tecnico di CA
     - Video di YouTube (predefinito)

5. Fare clic su Salva.

Le preferenze generali vengono salvate.

Definizione degli avvisi di posta elettronica

CA ARCserve Central Protection Manager consente di specificare le preferenze per gli avvisi di posta elettronica.

Per definire gli avvisi di posta elettronica

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la finestra di dialogo Nuovo criterio.

3. Selezionare la scheda Preferenze, quindi fare clic su Avvisi di posta elettronica.

   Verrà visualizzata la finestra di dialogo Preferenze - Avvisi di posta elettronica.

4. Specificare gli avvisi di posta elettronica desiderati.

   - **Abilita avvisi di posta elettronica** - Selezionare questa opzione per abilitare la preferenze su questa schermata.
   - **Impostazioni di posta elettronica** - Fare clic su questo pulsante per aprire la finestra di dialogo corrispondente (a pagina 132).
   - **Notifiche** - Indica se inviare automaticamente notifiche di avviso di posta elettronica al completamento di eventi selezionati. È possibile selezionare una o tutte le opzioni disponibili.

     Tali opzioni consentono di inviare una notifica di avviso per i seguenti eventi:

     Avvisi del processo di backup

     – **Processi non eseguiti** - Invia una notifica di posta elettronica di avviso per tutti i processi non eseguiti. Per processo non eseguito, si intenderà qualunque processo pianificato non eseguito all'ora stabilita. Questo problema può verificarsi quando un altro processo è in esecuzione o un processo precedente non è stato completato quando previsto. Ad esempio, se un processo di esportazione o di recupero è in esecuzione nel momento in cui dovrebbe avvenire l'esecuzione di un processo di backup pianificato, tale processo di backup non verrà eseguito.

     – **Errore o arresto anomalo durante i processi di backup, catalogo, copia file, ripristino o copia del punto di ripristino** - Invia una notifica di avviso di posta elettronica in caso di errore dei processi di backup, catalogo, copia file, ripristino e copia del punto di ripristino. Questa categoria include tutti i processi non riusciti, incompleti, annullati, non eseguiti e i tentativi terminati con un arresto anomalo.

     – **Completamento dei processi di backup, catalogo, copia file, ripristino o copia del punto di ripristino** - Invia una notifica di avviso di posta elettronica in seguito al completamento dei processi di backup, catalogo, copia file, ripristino e copia del punto di ripristino.

     – **Processo di unione interrotto, ignorato, non riuscito o arrestato in modo anomalo** - Viene inviata una notifica di avviso a tutti i processi interrotti, ignorati, non riusciti o arrestati in modo anomalo. Se questo avviso viene abilitato, l'utente verrà informato quando un processo di unione non viene completato. Un errore di unione può verificarsi per i seguenti motivi: la sessione viene montata, la sessione viene bloccata da un processo di catalogo, oppure la sessione è bloccata per altri motivi.

     – **Processo di unione eseguito correttamente** - Invia un messaggio di avviso per tutti i processi di unione completati correttamente.

Avvisi di spazio su disco

- **Lo spazio libero sulla destinazione di backup è inferiore al** - Viene inviata una notifica di avviso nel caso in cui la quantità di spazio inutilizzato nella destinazione di backup è inferiore al valore specificato. Per questa opzione, è possibile selezionare una percentuale della capacità totale o un valore specifico (in MB) indicante il livello limite a partire dal quale inviare le notifiche di avviso.

Avvisi di aggiornamento

- **Nuovi aggiornamenti disponibili** - Viene inviata una notifica di avviso se è disponibile un nuovo aggiornamento di CA ARCserve D2D. Le notifiche di posta elettronica verranno inviate anche in caso di errore durante la verifica degli aggiornamenti o durante il download.

Avvisi sulle risorse

- **Abilita avvisi sulle risorse** - Invia una notifica di posta elettronica quando viene raggiunta la soglia specificata per l'indicatore di prestazioni chiave (PKI). Per garantire che i server siano efficienti e affidabili, è necessario un controllo continuo delle prestazioni per identificare possibili problemi e rispondere velocemente a situazioni di arresto.

  La definizione dei livelli soglia per gli indicatori di prestazioni è discrezionale e dipende dal livello di conoscenza del proprio server. Non esistono impostazioni giuste o sbagliate. Le notifiche di avviso dovrebbero essere basate su prestazioni "normali" ed accettabili. Ad esempio, se il sistema normalmente viene eseguito con un carico CPU dell'80%, impostare la soglia di utilizzo della CPU sul 75% risulterebbe poco utile o efficace.

  Ciascuno parametro PKI può essere configurato individualmente per l'invio di una notifica di avviso quando viene raggiunto il livello soglia corrispondente all'indicatore. Il numero massimo di messaggi di posta elettronica di avviso per PKI è di 5 al giorno.

- **Utilizzo CPU** - La soglia di avviso specificata per l'utilizzo della CPU indica la percentuale di utilizzo CPU del server protetto CA ARCserve D2D. È possibile utilizzare una notifica di avviso per assicurarsi che il server non raggiunga troppo spesso uno stato di sovraccarico.

  Se l'uso della CPU è eccessivo, il tempo di risposta del server potrebbe diventare molto lento o addirittura inesistente, con la necessità di prendere in considerazione la distribuzione del carico (bilanciamento).

- **Velocità del disco** - La soglia di avviso specificata per la velocità del disco indica la velocità del disco (MB/secondo) del server protetto CA ARCserve D2D. È possibile utilizzare la notifica di avviso per verificare il livello di sfruttamento delle capacità del disco.

Se la velocità del disco è vicina al valore massimo che il disco può gestire, è necessario considerare l'aggiornamento a un disco che soddisfi meglio le proprie esigenze. In genere un disco più veloce porta a prestazioni migliori.

- **Utilizzo memoria** - La soglia di avviso specificata per l'utilizzo della memoria indica la percentuale di memoria in uso sul server protetto CA ARCserve D2D. L'utilizzo corrisponde al livello di capacità di memoria in uso. Più alta la percentuale, peggiori saranno le prestazioni del server.

  Se l'utilizzo della memoria risulta costantemente eccessivo, sarà necessario determinare il processo responsabile di tale utilizzo elevato. È possibile utilizzare questo indicatore per ricevere un avviso qualora dovesse essere necessario l'aggiornamento di un server o di un'applicazione.

- **I/O di rete** - La soglia di avviso specificata per l'I/O di rete indica la percentuale di ampiezza di banda della scheda di rete utilizzata sul server protetto CA ARCserve D2D. L'utilizzo fa riferimento al livello di capacità in uso della scheda di rete. Più alta la percentuale, peggiori saranno le prestazioni di rete.

  Se l'utilizzo della rete risulta costantemente eccessivo, sarà necessario determinare quale processo sta causando questo alto utilizzo e trovare una soluzione al problema. In aggiunta, se basandosi sulle capacità di rete specifiche la percentuale di utilizzo della rete è troppo alta durante il backup, potrebbe essere necessario effettuare l'aggiornamento della propria scheda NIC per gestire le esigenze di velocità effettiva più alte.

5. Fare clic su Salva.

Le opzioni di avviso di posta elettronica vengono salvate.

Definizione delle impostazioni di posta elettronica

La finestra di dialogo Impostazioni di posta elettronica inserisce automaticamente i valori correnti dal server di posta elettronica e dalla configurazione di posta elettronica del criterio nel nuovo criterio. Tali impostazioni sono valide per tutte le notifiche di avviso di posta elettronica e possono essere modificate in qualsiasi momento.

Servizio

Il servizio del provider di posta elettronica da utilizzare per l'invio delle notifiche di avviso. Le opzioni disponibili sono Google Mail, Yahoo Mail, Live Mail e altri.

- Se si seleziona Altro, sarà necessario identificare il server di posta e il numero di porta corrispondente da utilizzare come impostazione predefinita.
- Se si seleziona Google Mail, Yahoo Mail o Live Mail, i campi relativi al server di posta e al numero di porta vengono popolati automaticamente.

Server di posta elettronica

Il nome host del server di posta SMTP per l'invio degli avvisi di posta elettronica ci CA ARCserve D2D.

Porta

Il numero di porta di uscita del server di posta.

Richiede l'autenticazione

Indica se il server di posta elettronica richiede l'autenticazione per l'invio di un messaggio di posta elettronica via Internet. Se viene selezionata questa opzione, sarà necessario specificare il nome e la password dell'account utente corrispondenti.

Oggetto

Descrizione dell'oggetto per le notifiche di avviso di posta elettronica inviate da CA ARCserve D2D. Impostazione predefinita: Avviso CA ARCserve D2D.

Da

Indirizzo di posta elettronica utilizzato da CA ARCserve D2D per l'invio delle notifiche di avviso di posta elettronica.

Destinatari

Indirizzo di posta elettronica dei destinatari delle notifiche di avviso di posta elettronica.

Nota: per immettere più indirizzi di posta elettronica, è necessario separarli con un punto e virgola.

Usa SSL

Indica che il server di posta elettronica necessita di una connessione SSL (Secure Socket Layer) per la trasmissione protetta dei dati via Internet.

Invia STARTTLS

Indica che il server di posta elettronica richiede il comando STARTTLS (Start TLS extension) per l'inizializzazione di una connessione SMTP fra server.

Usa formato HTML

Indica che le notifiche di avviso di posta elettronica verranno inviate in formato HTML. Se questa opzione non viene selezionata, gli avvisi vengono inviati come testo normale. Questa opzione è selezionata per impostazione predefinita.

Abilita impostazioni proxy

Indica se si desidera stabilire la connessione a un server proxy per l'invio delle notifiche di posta elettronica di avviso. Se viene selezionata questa opzione, sarà necessario specificare il nome del server proxy e il numero di porta corrispondenti.

Messaggio di posta elettronica di verifica

Verifica che le impostazioni di configurazione della posta elettronica siano corrette.

Impostazione delle preferenze di aggiornamento

CA ARCserve Central Protection Manager consente di specificare le preferenze di aggiornamento.

Per definire le preferenze di aggiornamento

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Fare clic su Nuovo per creare un nuovo criterio.

   Verrà visualizzata la finestra di dialogo Nuovo criterio.

3. Selezionare la scheda Preferenze, quindi fare clic su Aggiorna.

   Verrà visualizzata la finestra di dialogo delle preferenze di aggiornamento.

4. Specificare le preferenze di aggiornamento.

   - **Server di download** - Indica il server di origine da cui CA ARCserve D2D scaricherà gli aggiornamenti disponibili.

     – **Server CA Technologies** - È possibile utilizzare questa opzione per impostare l'aggiornamento del download di CA ARCserve D2D dal server CA Technologies direttamente sul server locale.

     – **Server di gestione temporanea** - Questa opzione consente di specificare il server da utilizzare come server di gestione temporanea.

       Specificando più server di gestione temporanea, il primo server elencato verrà designato come server di gestione temporanea primario. Si tratta del primo server a cui CA ARCserve D2D cercherà di connettersi. Se per qualsiasi motivo il primo server elencato non fosse disponibile, il successivo server in elenco diventerà il server di gestione temporanea primario. La stessa sequenza verrà mantenuta fino a quando l'ultimo server elencato diventerà il server di gestione temporanea primario. L'elenco dei server di gestione temporanea è limitato a un massimo di cinque server.

     – Utilizzare i pulsanti Sposta su e Sposta giù per modificare la sequenza dei server di gestione temporanea.

     – Utilizzare il pulsante Elimina per rimuovere un server dall'elenco.

     – Utilizzare il pulsante Aggiungi server per aggiungere un nuovo server all'elenco. Facendo clic sul pulsante Aggiungi server, verrà visualizzata la finestra di dialogo Server di gestione temporanea, dalla quale sarà possibile specificare il nome del server di gestione temporanea aggiunto e il numero di porta, che per impostazione predefinita è impostato sul numero di porta corrente dell'utente.

       Si tratta dell'impostazione predefinita.

       Nota: per i criteri D2D, il server di gestione temporanea predefinito corrisponde al computer CA ARCserve Central Applications locale.

       Gli aggiornamenti di CA ARCserve D2D vengono scaricati dal server CA Technologies direttamente sulla posizione del server di gestione temporanea specificata. Dopo il download degli aggiornamenti sul server di gestione temporanea, sarà possibile scaricare tali aggiornamenti dal server di gestione temporanea su un server client. Se si seleziona il percorso del server di gestione temporanea, sarà necessario specificare anche il nome host o l'indirizzo IP di tale server con il numero di porta corrispondente.

- **Impostazioni proxy** - Queste impostazioni sono disponibili solo se si seleziona il server CA come server di download.

  Fare clic su Impostazioni proxy per indicare se si desidera che gli aggiornamenti di CA ARCserve D2D vengano scaricati attraverso un server proxy. Le impostazioni immesse verranno utilizzate per la connessione al server CA dal quale il server di download acquisirà gli aggiornamenti.

  Facendo clic su questo pulsante, verrà visualizzata la finestra di dialogo delle impostazioni proxy.

- **Utilizza le impostazioni proxy del browser (solo per IE e Chrome)** - Consente di utilizzare le credenziali immesse per il proxy CA ARCserve D2D.
- **Configura impostazioni proxy** - Un server proxy funge da intermediario tra il server di download (di gestione temporanea o client) e il server CA, al fine di garantire la protezione, le prestazioni e il controllo amministrativo. Per impostazione predefinita, questa opzione è disabilitata.

  Selezionare l'opzione se si desidera utilizzare un server proxy per la connessione al server CA da cui scaricare le informazioni di aggiornamento di CA ARCserve D2D. Il server proxy si connetterà direttamente al server CA per acquisire le informazioni di aggiornamento. Abilitando questa opzione, sarà necessario includere anche l'indirizzo IP (o il nome host) del server proxy e il numero di porta per la connessione utilizzati dal server proxy per la connessione.

  Se l'opzione non viene selezionata, il server di download si connetterà direttamente al server CA senza passare per un server proxy.

  Inoltre, sarà possibile specificare se il server proxy richiede l'autenticazione. Se selezionata, infatti, l'opzione indica che sono necessarie informazioni di autenticazione (ID utente e password) per l'utilizzo del server proxy.

- **Verifica connessione** - Consente di verificare le seguenti connessioni e visualizzare un messaggio di stato al completamento.
  - Se è stato selezionato il server CA Technologies come server di download, viene verificata la connessione tra il computer e il server CA Technologies attraverso il server proxy specificato.
  - Se è stato selezionato il server di gestione temporanea come server di download, viene verificata la connessione tra il computer e il server di gestione temporanea specificato.

    Il pulsante Verifica connessione viene utilizzato per verificare la disponibilità di ciascun server di gestione temporanea in elenco. Lo stato del server viene visualizzato nel campo Stato connessione.

  Nota: la verifica della connessione viene eseguita automaticamente all'avvio della finestra di dialogo delle preferenze di aggiornamento automatico quando viene creato un nuovo criterio.

- **Pianificazione aggiornamento** - Indica quando verificare la presenza (e scaricare) eventuali nuovi aggiornamenti di CA ARCserve D2D.

  Se questa opzione è stata selezionata, viene effettuata la verifica automatica dei nuovi aggiornamenti di CA ARCserve D2D disponibili. Selezionando questa opzione, vengono visualizzate le opzioni del menu a discesa che consentono di definire quando eseguire questa funzione (ogni giorno oppure ogni settimana in un giorno specifico) e l'ora del giorno in cui eseguirle.

  Se l'opzione viene selezionata senza specificare un giorno e un'ora, la pianificazione predefinita di verifica automatica è impostata su ogni domenica alle ore 4:00.

  Qualora risultassero disponibili nuovi aggiornamenti, CA ARCserve D2D procederà automaticamente al download. Se non si desidera scaricare gli aggiornamenti automaticamente, è possibile disattivare la funzionalità dal file D2DPMSettings.INI. Per ulteriori informazioni, consultare Guida per l'utente di CA ARCserve D2D sul sito Web del CA Support. https://support.ca.com/cadocs/0/CA%20ARCserve%20D2D%20r16-ENU/Bookshelf.html

  Se l'opzione non viene selezionata, le funzionalità di verifica e di download automatico vengono disabilitate e il loro stato compare nella sezione di riepilogo della pagina principale.

  Queste funzionalità di aggiornamento possono essere attivate solo manualmente.

  Nota: se configurate, si riceveranno notifiche di posta elettronica quando la verifica pianificata rileva la presenza di nuovi aggiornamenti. Inoltre, si riceveranno notifiche di posta elettronica anche in caso di errori durante la verifica o il download degli aggiornamenti.

5. Fare clic su Salva.

Le preferenze di aggiornamento vengono salvate.

Modifica o copia di criteri

CA ARCserve Central Protection Manager consente di modificare o copiare i criteri dopo averli creati.

Per modificare i criteri

1. Accedere all'applicazione.

   Fare clic su Criteri nella barra di navigazione per accedere alla schermata Criteri.

2. Dalla schermata Criteri, fare clic sulla casella di controllo corrispondente al criterio, quindi eseguire una delle seguenti operazioni:

   - Fare clic su Modifica della barra degli strumenti per modificare il criterio selezionato.
   - Fare clic su Copia della barra degli strumenti per copiare e creare un nuovo criterio dal criterio selezionato.

     Nota: la finestra di dialogo Copia criterio viene visualizzata quando viene eseguita la copia di un criterio. Specificare un nuovo nome per il criterio e fare clic su OK.

   Verrà visualizzata la finestra di dialogo Modifica criterio.

3. Se si desidera modificare il nome del criterio, specificare un nome nel campo Nome criterio.
4. Specificare i valori richiesti e fare clic su Salva.

Il criterio viene modificato o copiato.

Eliminazione dei criteri

CA ARCserve Central Protection Manager consente di eliminare i criteri creati precedentemente.

Nota: CA ARCserve Central Protection Manager non consente l'eliminazione dei criteri assegnati ai nodi. Per eliminare i criteri a cui sono assegnati nodi, è necessario annullare l'assegnazione dei nodi dal criterio, quindi eliminare il criterio. Per informazioni sull'annullamento dell'assegnazione dei nodi da un criterio, consultare la sezione Assegnazione e annullamento dell'assegnazione di nodi dai criteri (a pagina 140).

Per eliminare i criteri

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Dall'elenco Criteri, fare clic sul criterio che si desidera eliminare.

3. Fare clic su Elimina della barra degli strumenti Criteri.

   Verrà visualizzato un messaggio di conferma di eliminazione.

4. Fare clic su Sì per eliminare il criterio.

   Nota: se un criterio viene eliminato per sbaglio, sarà necessario creare nuovamente il criterio. Se non si desidera eliminare il criterio, fare clic su No.

Il criterio viene eliminato.

Distribuzione dei criteri

CA ARCserve Central Protection Manager consente di effettuare la distribuzione dei criteri nel caso in cui la distribuzione sia stata eseguita più volte o non sia stata completata su server remoti.

Per effettuare la distribuzione di criteri

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri nella barra di navigazione.

   Viene visualizzata la schermata Criteri.

2. Selezionare un criterio dall'elenco Criteri, quindi fare clic su Distribuisci ora.

   Il criterio viene distribuito immediatamente.

Nota: quando il criterio viene distribuito correttamente a un nodo CA ARCserve D2D, le impostazioni del nodo CA ARCserve D2D non potranno essere modificate. Ad eccezione dell'attivazione del pulsante Aggiorna connessione, CA ARCserve D2D è in grado di eseguire la risincronizzazione delle informazioni sulla connessione nella destinazione di backup se le credenziali di accesso sono state modificate sul server remoto. Inoltre, è possibile visualizzare lo stato di distribuzione dei criteri dalla schermata Elenco nodi della colonna Criterio.

Assegnazione e annullamento dell'assegnazione di nodi dai criteri

CA ARCserve Central Protection Manager consente di assegnare o annullare l'assegnazione di un nodo dai criteri D2D esistenti.

Procedere come descritto di seguito:

1. Dalla pagina principale di CA ARCserve Central Protection Manager, selezionare Criteri dalla barra di navigazione per accedere alla schermata Criteri.
2. Selezionare un criterio dall'elenco corrispondente, quindi fare clic sulla scheda Assegnazione criterio.

   Verrà visualizzato un elenco dei nodi assegnati al criterio selezionato con uno dei seguenti stati di distribuzione e azioni (Formato: *[azione] stato di distribuzione*):

   - [Assegna] In sospeso
   - [Annulla assegnazione] Distribuzione in corso
   - [Risincronizzazione] Completato
   - [Aggiornamento] Non riuscito
   - [Ridistribuisci] Distribuzione di D2D eseguita correttamente
   - [Ridistribuisci] Distribuzione di D2D non riuscita
   - [Ridistribuisci] Riavvio della distribuzione D2D
3. Fare clic sul pulsante Assegnazione e annullamento assegnazione.

   Verrà visualizzata la finestra di dialogo Assegna/Annulla assegnazione criterio.
4. Specificare i campi seguenti nella finestra di dialogo Assegnazione/Annullamento assegnazione criterio:

   - **Gruppo:** selezionare il nome del gruppo contenente i nodi da assegnare.
   - **Filtro Nome nodo:** consente di filtrare i nodi disponibili in base a un criterio comune.

     Nota: il campo Nome nodo consente di filtrare i nodi mediante caratteri jolly.

     Ad esempio, Acc* consente di filtrare tutti i nodi il cui nome inizia per Acc. Per cancellare i risultati del filtro, fare clic su sul simbolo X del campo Filtro.

5. Effettuare una delle seguenti operazioni:

   - **Assegnazione di nodi ai criteri:** selezionare i nodi che si desidera aggiungere e fare clic sulla freccia destra singola.

     I nodi verranno spostati dall'elenco Nodi selezionati all'elenco Nodi selezionati.

     Nota: per selezionare e spostare tutti i nodi, fare clic sulla freccia destra doppia.

   - **Annullamento dell'assegnazione dei nodi dai criteri:** selezionare i nodi di cui si desidera annullare l'assegnazione, quindi fare clic sulla freccia sinistra singola.

     I nodi verranno spostati dall'elenco Nodi selezionati all'elenco Nodi disponibili.

     Nota: per selezionare e spostare tutti i nodi, fare clic sulla freccia sinistra doppia.

   Fare clic su OK.

   Nota: il seguente messaggio viene visualizzato durante l'annullamento dell'assegnazione dei nodi:

   ```
   You are unassigning the policies from the selected node.(Annullamento
   dell'assegnazione dei criteri dal nodo selezionato.) You can keep the current
   settings to allow the node to continue the backup process. ( È possibile
   mantenere le impostazioni correnti per consentire ai nodi di procedere con il
   processo di backup.) Do you want to keep the settings? (Mantenere le
   impostazioni?) Fare clic su Sì per mantenere le impostazioni correnti di
   CA ARCserve D2D, fare clic su No per rimuovere le impostazioni di
   CA ARCserve D2D attuali, oppure selezionare Annulla per tornare alla
   schermata Assegnazione/Annullamento assegnazione criterio.
   ```

   Se si seleziona No, le impostazioni remote di CA ARCserve D2D verranno perse e il server CA ARCserve D2D non verrà protetto.

I nodi vengono applicati ai criteri specificati.

Esecuzione di un backup immediato

In genere, i backup vengono eseguiti automaticamente e vengono controllati attraverso le impostazioni di pianificazione. Ad ogni modo, potrebbe essere necessario eseguire un backup ad hoc immediato (completo, incrementale o di verifica).

Il backup ad hoc viene eseguito a seconda delle esigenze, e non viene pianificato come parte di un piano di backup. Ad esempio, se sono stati pianificati backup completi, incrementali e di verifica e si desidera apportare modifiche sostanziali al computer, sarà necessario eseguire un backup ad hoc immediato senza attendere l'esecuzione del backup pianificato successivo.

Un backup ad hoc consente inoltre di aggiungere un punto di ripristino personalizzato (non pianificato) per tornare al punti precedente specificato, in qualsiasi momento.. Ad esempio, se si procede all'installazione di una patch o di un service pack e, successivamente, si rileva che tale installazione influenza le prestazioni del computer, potrebbe essere necessario eseguire un ripristino utilizzando la sessione di backup ad hoc precedente all'installazione.

Procedere come descritto di seguito:

1. Accedere all'applicazione.
2. Dalla barra di navigazione della pagina principale, fare clic su Nodo per aprire la schermata Nodo.
3. Eseguire una delle azioni seguenti per specificare i nodi di cui si desidera eseguire il backup:
   - **Livello di nodo:** fare clic sul gruppo contenente i nodi di cui si desidera eseguire il backup e selezionare la casella di controllo corrispondente.
   - **Livello di gruppo:** fare clic sul gruppo contenente i nodi di cui si desidera eseguire il backup.
4. Effettuare quindi una delle azioni seguenti per eseguire il backup del nodo:
   - Fare clic su Backup dalla barra degli strumenti.
   - Fare clic con il tasto destro del mouse sul gruppo o sui nodi selezionati, quindi fare clic sul Esegui backup dal menu di scelta rapida.

5. Nella finestra di dialogo Esecuzione di un backup immediato, specificare il tipo di backup selezionando uno dei tipi seguenti:

   - **Backup completo -** Avvia un backup completo di tutto il computer o dei volumi selezionati.
   - **Backup incrementale -** Avvia un backup incrementale del computer. Un backup incrementale esegue il backup solo dei blocchi modificati dopo l'ultimo backup.

     Nota: i backup incrementali presentano il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. Questa modalità di esecuzione backup è ottimale.

   - **Backup di verifica -** Avvia un backup di verifica del computer analizzando il backup più recente di ciascun singolo blocco e ne confronta il contenuto e le informazioni con l'origine iniziale. Questo confronto consente di verificare che le informazioni corrispondenti all'origine siano contenute nel blocco di backup più recente. Se l'immagine di backup di un determinato blocco non corrisponde all'origine, CA ARCserve D2D aggiornerà (risincronizzerà) il backup di tale blocco. L'esecuzione di un backup di verifica presenta i seguenti vantaggi e svantaggi:

     – Vantaggio: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.

     – Svantaggio: la velocità del tempo di backup è ridotta in quanto i blocchi di backup originali vengono confrontati con i blocchi di backup più recenti.

   Nota: se si aggiunge un nuovo volume all'origine di backup, il volume appena aggiunto verrà sottoposto a un backup completo, indipendentemente dal metodo di backup generale utilizzato.

6. (Facoltativo) Specificare un nome di backup e fare clic su OK. Se non viene specificato un nome, il backup verrà utilizzato il nome predefinito Customized/Full/Incremental/Verify Backup.

Verrà visualizzata una finestra di dialogo di conferma e il tipo di backup selezionato verrà avviato automaticamente.

Tenere presenti le seguenti considerazioni:

- Tutti i valori specificati nelle finestre di dialogo Criterio verranno applicati al processo.
- In caso di errore di un processo di backup (ad hoc) personalizzato, non verrà creato alcun processo di composizione. I processi di riparazione vengono creati solo in caso di errore di processi pianificati.

Visualizzazione delle informazioni sullo stato del processo,

nonché visualizzare informazioni dettagliate sul processo. Se lo si desidera, è possibile interrompere un processo in corso di esecuzione.

Procedere come descritto di seguito:

1. Accedere all'applicazione.
2. Dalla barra di navigazione della pagina principale, fare clic su Nodo per aprire la schermata Nodo.
3. Nella struttura Gruppi, selezionare il gruppo contenente il nodo per cui si desidera visualizzare lo stato del processo.

   Se il processo è in corso, la fase del processo viene visualizzata nella colonna Processo.

4. Fare clic sulla fase mostrata nella colonna Processo per accedere alla finestra di dialogo Monitoraggio dello stato di backup.
5. Nella finestra di dialogo Monitoraggio dello stato di backup, eseguire una delle operazioni seguenti:
   - Fare clic su Chiudi per chiudere la finestra di dialogo Monitoraggio dello stato di backup.
   - Fare clic su Annulla per interrompere il processo corrente.

     Nota: la finestra di dialogo Monitoraggio dello stato di backup verrà chiusa qualche secondo dopo aver selezionato Annulla.

Modalità di ripristino dei nodi in CA ARCserve Central Protection Manager

CA ARCserve Central Protection Manager fornisce diversi strumenti e opzioni per il ripristino dei nodi. In questa sezione vengono fornite informazioni su come ripristinare i dati in modo sicuro ed efficace.

Questa sezione contiene i seguenti argomenti:

Ripristino dei dati dai punti di ripristino

L'opzione Sfoglia punti di ripristino consente di ripristinare qualsiasi applicazione individuando i punti di ripristino disponibili (backup completati con successo) da un calendario.

Per ripristinare i dati dai punti di ripristino

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.
2. Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.

3. Nella finestra di dialogo Ripristino, fare clic su Sfoglia punti di ripristino.

   Verrà visualizzata la finestra di dialogo Sfoglia punti di ripristino.

4. Indicare la posizione di backup oppure accedere al percorso di archiviazione delle le immagini di backup.

   Nota: per convalidare la connessione alla destinazione di backup specificata, fare clic sulla freccia verde accanto al pulsante Sfoglia. Per la connessione a una condivisione di rete remota, potrebbe essere necessario immettere il nome utente e la password.

   La visualizzazione calendario evidenzia in verde tutte le date che contengono punti di ripristino per l'origine di backup specificata all'interno del periodo di tempo visualizzato.

5. Specificare le informazioni per il ripristino.

   a. Nel calendario, selezionare la data dell'immagine di backup da ripristinare.

      Verranno visualizzati i punti di ripristino per tale data, con informazioni sull'ora di backup, il tipo di backup eseguito, il nome del backup e lo stato del catalogo.

   b. Selezionare un punto di ripristino.

      Verrà visualizzato il contenuto del backup (eventuali applicazioni incluse) per il punto di ripristino selezionato.

   c. Selezionare il contenuto da ripristinare.

      - Nei ripristini a livello di volume, è possibile selezionare l'intero volume oppure solo alcuni file o cartelle del volume.

      - Per un ripristino a livello di applicazione, è possibile scegliere di ripristinare l'intera applicazione o solo determinati componenti, database, istanze, ecc. dell'applicazione.

   Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

6. Selezionare la destinazione per il ripristino.

   Le opzioni disponibili consentono di eseguire il ripristino nella posizione originale del backup, oppure di eseguire il ripristino in una posizione diversa.

   Ripristina in posizione originale

   Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

   Nota: durante il ripristino della cartella dei registri di CA ARCserve D2D nella posizione originale, i file contenuti in tale cartella vengono ignorati. Per CA ARCserve Central Host-Based VM Backup, questa opzione è disattivata per impostazione predefinita. Per utilizzarla, installare CA ARCserve D2D nel sistema operativo guest e quindi eseguire il ripristino.

   Ripristina su:

   È possibile specificare una posizione oppure raggiungere il percorso in cui dovrà essere eseguito il ripristino delle immagini di backup. Per verificare la connessione al percorso specificato, fare clic sulla freccia verde.

   Potrebbe essere necessario immettere le credenziali Nome utente e Password per potere accedere al percorso.

7. Indicare la modalità di risoluzione dei conflitti riscontrati durante il processo di ripristino.

   Le opzioni disponibili sono:

   Sovrascrivi i file esistenti

   Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dal file di backup, indipendentemente dalla loro presenza sul computer.

   Sostituisci file attivi

   Consente di sostituire i file attivi dopo il riavvio. Se durante il tentativo di ripristino CA ARCserve D2D rileva che il file esistente è momentaneamente in uso, tale file non verrà sostituito immediatamente. Per evitare l'insorgere di problemi, i file attivi verranno sostituiti al successivo riavvio del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita al riavvio successivo).

   Nota: se questa opzione non viene selezionata, tutti i file attivi verranno ignorati dal processo di ripristino.

   Rinomina file

   Se il nome file esiste già, consente di creare un nuovo file. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno quindi ripristinati nel nuovo file.

   Ignora file esistenti

   Ignora e non sovrascrive (sostituisce) i file esistenti contenuti nella destinazione di ripristino. Verrà eseguito soltanto il ripristino dai file di backup degli oggetti non esistenti sul computer.

   Questa opzione è selezionata per impostazione predefinita.

8. (Facoltativo) Selezionare Crea directory principale dalla struttura directory.

   In tal modo, sarà possibile ricreare la stessa struttura di directory principale nel percorso della destinazione di ripristino.

   Nota: se questa opzione non viene selezionata, il file o la cartella selezionati vengono ripristinati direttamente nella cartella di destinazione.

9. Immettere la password di crittografia del backup per ripristinare i dati codificati quindi fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

10. Verificare che le opzioni di ripristino e le impostazioni siano corrette.

    – Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.

Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

Ripristino da copie di file

L'opzione Sfoglia copie file consente di eseguire il recupero dei dati dalle copie di file di CA ARCserve D2D. Le copie di file sono copie dei punti di ripristino di CA ARCserve D2D eseguite su supporti di archiviazione non in linea, quali dischi o cloud. Dalle copie di file è possibile specificare i dati che si desidera recuperare.

Per eseguire il ripristino da copie di file

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.
2. Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.
3. Dalla finestra di dialogo Ripristino, fare clic su Sfoglia copie file.

   Viene visualizzata la finestra di dialogo Sfoglia copie file.
4. Nel riquadro Nome, specificare il dati di copia file che si desidera recuperare. È possibile specificare il volume oppure una combinazione qualsiasi di file e cartelle.

   Se si seleziona il ripristino di un solo file, nel riquadro a destra verranno visualizzate tutte le versioni copiate per tale file. Se sono disponibili più versioni, selezionare la versione di copia file desiderata.

   - **Modifica** - Consente di selezionare una posizione di archiviazione alternativa per le immagini di copia di file.

     Verrà visualizzata una finestra di dialogo contenente le opzioni di destinazione alternative disponibili.

     - **Unità locale o di rete** - Verrà visualizzata la finestra di dialogo di selezione della posizione di backup, che consente di individuare e selezionare una posizione alternativa su unità locali o di rete.
     - **Cloud** - Verrà visualizzata la finestra di dialogo Configurazione cloud, che consente di accedere e configurare una posizione cloud alternativa.

5. Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

6. Selezionare le seguenti opzioni nella finestra di dialogo Opzioni di ripristino:

   - **Destinazione** - Selezionare la destinazione di ripristino.
     - Ripristina in posizione originale - È possibile ripristinare i dati nella posizione di origine utilizzata per l'acquisizione dell'immagine di backup.
     - Ripristina su - È possibile specificare una posizione o individuare il percorso verrà eseguito il ripristino delle immagini di backup. Fare clic sulla freccia accanto al campo Ripristina per verificare la connessione alla posizione specificata.

       Potrebbe essere necessario immettere le credenziali Nome utente e Password per potere accedere al percorso.
   - **Risolvere Conflitti** - Specifica la modalità utilizzata da CA ARCserve D2D per la risoluzione dei conflitti rilevati durante il processo di ripristino.
     - Sovrascrivi i file esistenti - Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dal file di backup, indipendentemente dalla loro presenza sul computer.
     - Sostituisci file attivi - Sostituisce i file attivi al riavvio. Se durante il tentativo di ripristino CA ARCserve D2D rileva che il file esistente è in uso, tale file non verrà sostituito immediatamente. Per evitare eventuali problemi, i file attivi verranno sostituiti al successivo riavvio del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita al riavvio successivo).

       Nota: se l'opzione non è selezionata, i file attivi non verranno inclusi nel ripristino.
     - Rinomina file - Crea un nuovo file se il nome file è già esistente. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno ripristinati sul nuovo file.
     - Ignora file esistenti - Consente di ignorare e non sovrascrivere i file esistenti contenuti nella destinazione di ripristino. Verrà eseguito soltanto il ripristino dai file di backup degli oggetti non presenti sul computer.

       Questa opzione è selezionata per impostazione predefinita.

- **Struttura directory** - Specifica le operazioni che CA ARCserve D2D potrà eseguire nella struttura della directory durante il processo di ripristino.

  – Crea directory principale - Se l'immagine di backup acquisita contiene una struttura di directory principale, CA ARCserve D2D ricreerà la stessa struttura di directory nel percorso di destinazione di ripristino.

    Se l'opzione Crea directory principale non è selezionata, il file o la cartella da ripristinare verranno ripristinati direttamente nella cartella di destinazione.

    Esempio:

    Se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt e C:\Folder1\SubFolder2\B.txt e durante il ripristino è stata specificata la destinazione D:\Restore.

    Se si sceglie di ripristinare i file A.txt e B.txt individualmente, la destinazione dei file ripristinati corrisponderà a D:\Restore\A.txt e "D:\Restore\B.txt. La directory principale al di sopra del livello di file specificato non verrà ricreata.

    Se si sceglie di eseguire il ripristino a partire dal livello SubFolder2, la destinazione dei file ripristinati corrisponderà a D:\Restore\SubFolder2\A.txt e D:\Restore\SubFolder2\B.txt. La directory principale al di sopra del livello di cartella specificato non verrà ricreata.

    Se l'opzione Crea directory principale è selezionata, verrà ricreato l'intero percorso della directory principale per i file o le cartelle (compreso il nome del volume) nella cartella di destinazione. Se i file o le cartelle da ripristinare appartengono allo stesso nome del volume, il percorso della directory principale di destinazione non includerà tale nome del volume. Tuttavia, se i file o le cartelle da ripristinare appartengono a diversi nomi di volume, il percorso della directory principale di destinazione includerà il nome del volume.

    Esempio:

    Se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt, C:\Folder1\SubFolder2\B.txt, e E:\Folder3\SubFolder4\C.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

    Se si desidera ripristinare soltanto il file A.txt, la destinazione del file ripristinato corrisponderà a D:\Restore\ Folder1\SubFolder2\A.txt (verrà ricreata l'intera directory principale, eccetto il nome del volume).

    Se si esegue il ripristino di entrambi i file A.txt e B.txt, la destinazione dei file ripristinati corrisponderà a D:\Restore\C\Folder1\SubFolder2\A.txt e D:\Restore\E\Folder3\SubFolder4\C.txt (verrà ricreata l'intera directory principale, compreso il nome del volume).

- **Password di crittografia** - Se i dati del punto di ripristino selezionato sono crittografati, potrebbe essere necessario specificare la password di crittografia.

  Se il ripristino viene eseguito sullo stesso computer su cui è stato eseguito il backup crittografato, non sarà necessario immettere la password. La password verrà richiesta in caso di ripristino su un computer diverso.

  Nota: le icone riportate di seguito indicano se il punto di ripristino contiene informazioni crittografate e se è richiesta l'immissione di una password per il ripristino.

  Punto di ripristino non crittografato (icona orologio):

  Punto di ripristino crittografato (icona orologio con lucchetto).

Fare clic su Avanti.

Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

7. Verificare che le informazioni della finestra di dialogo Riepilogo di Ripristino siano corrette.

   Nota: se si desidera modificare le opzioni di ripristino specificate, fare clic su Indietro per tornare alla finestra di dialogo corrispondente.

   Fare clic su Fine.

Le opzioni di ripristino verranno applicate e verrà eseguito il recupero dei dati.

Ripristino di file e cartelle dai punti di recupero

Al completamento di ogni backup, tutti i file o le cartelle di cui è stato eseguito il backup vengono incluse nell'immagine snapshot del backup. Questo metodo di ripristino consente di specificare esattamente i file o le cartelle da ripristinare.

Per ripristinare file e cartelle dai punti di recupero

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.

   Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.

2. Dalla finestra di dialogo Ripristino, fare clic su Trova file/cartelle da ripristinare.

   Verrà visualizzata la finestra di dialogo Trova file/cartelle da ripristinare.

3. Specificare la posizione di backup e la posizione di copia file oppure individuare la posizione di archiviazione delle immagini di backup.

   Tenere presenti le seguenti considerazioni:

   - Per la posizione di backup, è possibile fare clic sulla freccia verde accanto al pulsante Sfoglia per confermare la connessione alla destinazione di backup specificata. Per la connessione a una condivisione di rete remota, potrebbe essere necessario immettere il nome utente e la password.
   - Per la posizione di copia file, è possibile fare clic sul pulsante Modifica per individuare un'unità di rete, locale oppure una destinazione cloud. Per ulteriori informazioni sulla posizione di copia file, consultare la sezione Ripristino da copie di file (a pagina 148).

4. Specificare il nome del file o della cartella da ripristinare.

   Nota: il campo Nome file supporta la ricerca per nome completo e con caratteri jolly. Se non si conosce il nome file completo, è possibile semplificare i risultati della ricerca immettendo i caratteri jolly "*" e "?" nel campo Nome file.

   I caratteri jolly supportati per il nome dei file o delle cartelle sono i seguenti:

   - "*" - Utilizzare l'asterisco per sostituire zero o più caratteri in un nome di file o directory.
   - "?" - Utilizzare il punto interrogativo per sostituire un singolo carattere nel nome di un file o di una directory.

   Ad esempio, specificando *.txt, la ricerca restituirà tutti i file con estensione .txt.

5. (Facoltativo) Specificare il nome di un percorso per filtrare ulteriormente la ricerca, indicando se includere o meno sottodirectory, file e cartelle.

6. Fare clic su Trova per dare inizio alla ricerca.

   Verranno visualizzati i risultati di ricerca. Se vengono rilevate più occorrenze (punti di ripristino) dello stesso file di ricerca, verranno elencate tutte le occorrenze in ordine cronologico (dalla più recente alla meno recente).

7. Selezionare la versione di cui si desidera eseguire il ripristino dall'elenco e fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

8. Selezionare la destinazione per il ripristino.

   Le opzioni disponibili consentono di eseguire il ripristino nella posizione originale del backup, oppure di eseguire il ripristino in una posizione diversa.

   Ripristina in posizione originale

   Esegue il ripristino dei dati nella posizione originale di acquisizione dell'immagine di backup.

   Nota: durante il ripristino della cartella dei registri di CA ARCserve D2D in posizione originale, i file contenuti in tale cartella verranno ignorati.

   Ripristina su:

   È possibile specificare una posizione oppure raggiungere il percorso in cui dovrà essere eseguito il ripristino delle immagini di backup. Per verificare la connessione al percorso specificato, fare clic sull'icona della freccia verde.

   Potrebbe essere necessario immettere le credenziali Nome utente e Password per potere accedere al percorso.

9. Indicare la modalità di risoluzione dei conflitti riscontrati durante il processo di ripristino.

   Le opzioni disponibili sono:

   Sovrascrivi i file esistenti

   Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dal file di backup, indipendentemente dalla loro presenza sul computer.

   Sostituisci file attivi

   Consente di sostituire i file attivi dopo il riavvio. Se durante il tentativo di ripristino CA ARCserve D2D rileva che il file esistente è momentaneamente in uso, tale file non verrà sostituito immediatamente. Per evitare l'insorgere di problemi, i file attivi verranno sostituiti al successivo riavvio del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita con il riavvio successivo).

   Nota: se questa opzione non viene selezionata, tutti i file attivi verranno ignorati dal processo di ripristino.

Rinomina file

Se il nome file esiste già, consente di creare un nuovo file. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno quindi ripristinati nel nuovo file.

Ignora file esistenti

Ignora e non sovrascrive (sostituisce) i file esistenti contenuti nella destinazione di ripristino. Solo gli oggetti inesistenti sul computer verranno ripristinati dai file di backup.

Questa opzione è selezionata per impostazione predefinita.

10. (Facoltativo) Selezionare Crea directory principale dalla struttura directory.

    In tal modo, sarà possibile ricreare la stessa struttura di directory principale nel percorso della destinazione di ripristino.

    Nota: se questa opzione non viene selezionata, il file o la cartella selezionati vengono ripristinati direttamente nella cartella di destinazione.

11. Immettere la password di crittografia del backup per ripristinare i dati codificati quindi fare clic su Avanti.

    Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

12. Verificare che le opzioni di ripristino e le impostazioni siano corrette.

    - Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.

Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

Ripristino dei dati da computer virtuali

Utilizzare l'opzione di ripristino del computer virtuale per eseguire il ripristino di un computer virtuale di cui è stato eseguito il backup in precedenza.

Per ripristinare dati da computer virtuali

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.

   Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.

2. Dalla finestra di dialogo Ripristino, fare clic su Recupera computer virtuale.

   Verrà visualizzata la finestra di dialogo di ripristino.

3. Specificare la posizione di backup di origine. È possibile specificare una posizione oppure individuare il percorso di archiviazione delle immagini di backup. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso. Fare clic sull'icona di convalida con la freccia verde per verificare che l'accesso alla posizione di origine sia stato eseguito correttamente.

   La visualizzazione calendario evidenzierà (in verde) tutte le date relative al periodo di tempo contenente i punti di ripristino per l'origine di backup selezionata.

4. Specificare il computer virtuale da ripristinare.

   Il menu a discesa includerà tutti i computer virtuali presenti nella posizione di backup specificata.

5. Selezionare la data corrispondente all'immagine del computer virtuale che si desidera ripristinare.

   Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito e al nome del backup.

6. Selezionare un punto di ripristino.

   Il contenuto del backup (incluse eventuali applicazioni) del punto di ripristino selezionato verrà visualizzato a scopo informativo. Durante il ripristino di un computer virtuale, verrà eseguito il ripristino dell'intero computer. Di conseguenza, sarà possibile visualizzare, ma non selezionare, singoli volumi, cartelle o file del computer virtuale selezionato.

   Nota: l'icona di un orologio con lucchetto indica che il punto di ripristino contiene informazioni crittografate e potrebbe richiedere una password per il ripristino.

7. Una volta completata la selezione delle informazioni di backup da ripristinare, fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

8. Selezionare la destinazione di ripristino.

   Ripristina in posizione originale

   Esegue il ripristino sul computer virtuale nel percorso in cui è stata acquisita l'immagine di backup. Questa opzione è selezionata per impostazione predefinita.

   Per ulteriori informazioni, consultare la sezione Ripristino del computer virtuale in posizione originale.

   Ripristino in una posizione alternativa

   Esegue il ripristino sul computer virtuale in un percorso diverso da quello in cui è stata acquisita l'immagine di backup.

   Per ulteriori informazioni, consultare la sezione Ripristino del computer virtuale in una posizione alternativa.

9. Specificare la modalità di risoluzione di eventuali conflitti riscontrati durante il processo di ripristino.

   Indicare, quindi, se si desidera sovrascrivere il computer virtuale esistente. Per impostazione predefinita, l'opzione di sovrascrittura non è selezionata.

   - Selezionando l'opzione, il processo di ripristino sovrascriverà (sostituirà) le immagini esistenti del computer virtuale che risiedono sulla destinazione di ripristino specificata. L'immagine del computer virtuale verrà ripristinata dai file di backup indipendentemente dalla sua presenza sulla destinazione di ripristino.
   - Se l'opzione non viene selezionata, il processo di ripristino procederà alla creazione di una nuova immagine del computer virtuale (senza sovrascrivere le immagini esistenti) sulla destinazione di ripristino specificata.

10. Specificare l'opzione Post-recupero.

    Indicare se si desidera attivare il computer virtuale al termine del processo di ripristino. Per impostazione predefinita, l'opzione di attivazione del computer virtuale non è selezionata.

Ripristino di computer virtuali nella posizione originale

Durante il processo di configurazione del ripristino del computer virtuale, è necessario selezionare la posizione in cui di desidera ripristinare il computer virtuale. Le opzioni disponibili sono Ripristina in posizione originale e Ripristina in posizione alternativa.

Se si seleziona per il ripristino del computer virtuale in posizione originale, attenersi ai seguenti passaggi:

Per ripristinare computer virtuali nella posizione originale

1. Dalla finestra di dialogo Opzioni di ripristino, dopo aver specificato le opzioni Risolvi conflitti e Post-recupero, selezionare l'opzione Ripristina in posizione originale, quindi fare clic su Avanti.

   Nota: per ulteriori informazioni sulle opzioni Risolvi conflitti e Post-recupero, consultare la sezione Ripristino dei dati da computer virtuali (a pagina 154).

   Verrà visualizzata la finestra di dialogo di impostazione delle credenziali per il server Vcenter/ESX di origine.

2. Specificare le credenziali di accesso al computer virtuale.
   - **Server vCenter/ESX** - Specifica il nome host o l'indirizzo IP del sistema server vCenter o ESX di destinazione.
   - **Nome del computer virtuale** - Specifica il nome host del computer virtuale di cui si sta eseguendo il ripristino.
   - **Protocollo -** Specifica il protocollo da utilizzare per la comunicazione con il server di destinazione. Le opzioni disponibili sono HTTP e HTTPS.
   - **Numero di porta -** Specifica la porta da utilizzare per il trasferimento dei dati tra il server di origine e il server di destinazione. Per impostazione predefinita, il numero di porta è 443.
   - **Nome utente** - Consente di specificare il nome dell'utente che dispone dell'autorizzazione per l'accesso al computer virtuale da ripristinare.
   - **Password** - Specifica la password corrispondente al nome utente richiesto per l'accesso al computer virtuale di cui si sta eseguendo il ripristino.
3. Dopo aver specificato le credenziali, fare clic su OK.

   Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.
4. Verificare che le opzioni di ripristino e le impostazioni siano corrette.
   - Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
   - Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

Ripristino di computer virtuali in posizioni alternative

Durante il processo di configurazione del ripristino del computer virtuale, è necessario selezionare la posizione in cui di desidera ripristinare il computer virtuale. Le opzioni disponibili sono Ripristina in posizione originale e Ripristina in posizione alternativa.

Se si desidera ripristinare il computer virtuale in una posizione alternativa, procedere come segue:

Per ripristinare computer virtuali in posizioni alternative

1. Dalla finestra di dialogo Opzioni di ripristino, dopo aver specificato le opzioni Risolvi conflitti e Post-recupero, selezionare l'opzione Ripristina in posizione alternativa.

   Nota:per ulteriori informazioni sulle opzioni Risolvi conflitti e Post-recupero, consultare la sezione Recupero dei dati su computer virtuali (a pagina 154).

   La finestra di dialogo Opzioni di ripristino verrà espansa per visualizzare ulteriori opzioni di ripristino in posizione alternativa.

2. Specificare le informazioni del server vCenter/ESX.

   - **Server vCenter/ESX** - Specifica il nome host o l'indirizzo IP del sistema server vCenter o ESX di destinazione.
   - **Nome utente** - Consente di specificare il nome dell'utente che dispone dei privilegi di accesso per il computer virtuale da ripristinare.
   - **Password** - Specifica la password corrispondente al nome utente richiesto per l'accesso al computer virtuale di cui si sta eseguendo il ripristino.
   - **Protocollo -** Specifica il protocollo da utilizzare per la comunicazione con il server di destinazione. Le opzioni disponibili sono HTTP e HTTPS.
   - **Numero di porta -** Specifica la porta da utilizzare per il trasferimento dei dati tra il server di origine e il server di destinazione. Per impostazione predefinita, il numero di porta è 44.

3. Dopo aver specificato le informazioni del server vCenter/ESX, fare clic sul pulsante Connetti a questo server vCenter/ESX.

   Se le informazioni per l'accesso al server alternativo sono corrette, verrà abilitato il campo Ulteriori informazioni.

4. Immettere le informazioni richieste.

   - **Nome del computer virtuale** - Specifica il nome host del computer virtuale di cui si sta eseguendo il ripristino.
   - **Server ESX** - Specifica il server ESX di destinazione. Il menu a discesa contiene un elenco di tutti i server ESX associati al computer virtuale specificato.
   - **Archivio dati del computer virtuale** - Consente di specificare la destinazione di archiviazione del computer virtuale.

5. Dopo aver immesso tutte le informazioni necessarie, fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

6. Verificare che le opzioni di ripristino e le impostazioni siano corrette.

   - Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
   - Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

Ripristino dei dati di posta elettronica di Microsoft Exchange

Quando un backup di CA ARCserve D2D viene completato con successo, viene creata un'immagine snapshot temporizzata del backup. L'insieme dei punti di ripristino consente di individuare e specificare esattamente le immagini di backup da ripristinare. Per Microsoft Exchange Server, è possibile sfogliare i punti di ripristino per individuare i singoli oggetti da ripristinare (caselle di posta, cartelle della casella di posta o messaggi). Per eseguire un ripristino granulare di Exchange, l'account deve disporre delle autorizzazioni necessarie. Per ulteriori informazioni, consultare la sezione Autorizzazioni di ripristino account di Exchange.

Nota: su Microsoft Exchange Server 2007 e versioni successive, l'API del sistema di messaggistica (MAPI) è un prerequisito necessario per il ripristino granulare di Exchange. Se non è installata, potrebbe non essere possibile eseguire ripristini granulari a livello di caselle di posta o messaggi. Per ulteriori informazioni sull'installazione dell'API del sistema di messaggistica su Exchange Server, fare riferimento all'Area download Microsoft.

Per eseguire il ripristino dei dati di posta elettronica di Microsoft Exchange

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.

   Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.

2. Dalla finestra di dialogo Ripristino, fare clic su Ripristina posta di Exchange.

   Verrà visualizzata la finestra di dialogo Ripristina posta di Exchange.

3. Specificare la posizione di backup. È possibile specificare una posizione oppure individuare il percorso di archiviazione delle immagini di backup. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso. Fare clic sulla freccia verde per verificare l'accesso alla posizione di origine.

   La visualizzazione calendario evidenzierà (in verde) tutte le date relative al periodo di tempo contenente i punti di ripristino per l'origine di backup selezionata.

4. Nel calendario, selezionare la data dell'immagine di backup da ripristinare.

   Verranno visualizzati, quindi, i database delle caselle di posta Exchange associati alla data, unitamente all'ora di backup, al tipo di backup eseguito e al nome del backup.

5. Selezionare un database delle caselle di posta di Exchange da ripristinare, quindi fare clic su Avanti.

   Nota: viene visualizzato un messaggio di notifica in cui viene chiesto se si desidera creare un catalogo di ripristino granulare di Exchange. Selezionando No, non sarà possibile sfogliare o selezionare un punto di ripristino granulare. Di conseguenza, sarà possibile eseguire esclusivamente un ripristino di database completo dalla finestra di dialogo Sfoglia punti di ripristino.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino, con un elenco dei contenuti della casella di posta per il database selezionato.

   Nota: è supportato solo il ripristino della posta elettronica. Non è supportato il ripristino del calendario, dei contatti, delle attività e delle note.

6. Selezionare il livello degli oggetti di Exchange da ripristinare (caselle di posta, cartelle o singoli messaggi).

   Nota: è possibile selezionare l'intero contenuto oppure parte del contenuto dell'oggetto di Exchange da ripristinare.

   a. Selezionare un database delle caselle di posta, per ripristinare tutte le caselle di posta di quel database.

   b. Selezionare il livello casella di posta, per ripristinare tutto il contenuto (cartelle e messaggi di posta) della casella di posta selezionata.

   c. Selezionare il livello cartella della casella di posta, per ripristinare tutto il contenuto di posta della cartella selezionata.

   d. Selezionare il livello messaggio singolo, per ripristinare solo l'oggetto di posta selezionato.

      Nota: in Exchange 2003, se i singoli messaggi da ripristinare sono stati inviati mediante un client di posta elettronica diverso da Outlook e il messaggio contiene un flag di stato al momento del backup, il messaggio verrà ripristinato, ma il flag non verrà incluso nel ripristino.

7. Fare clic su Avanti.
8. Selezionare la destinazione per il ripristino.

   Le opzioni disponibili consentono di eseguire il ripristino nella posizione originale del backup, oppure di eseguire il ripristino in una posizione diversa.

   Note:

   - Durante il ripristino di una casella o di un messaggio di posta (in posizione originale o alternativa), verificare che la destinazione sia disponibile, altrimenti il ripristino non potrà essere completato. CA ARCserve D2D convalida la destinazione solo quando il processo di ripristino viene inoltrato.
   - Se si tenta di ripristino dei messaggi di posta su un computer in cui gli indirizzi di posta elettronica di tali messaggi non sono validi (non esistono nel dominio) oppure se l'utente non ha effettuato l'accesso alla casella di posta, alcuni campi potrebbero essere visualizzati in modo diverso dopo il backup.
   - Su Exchange 2010, non è possibile procedere al ripristino in posizione originale degli elementi della casella di posta archiviati. Gli elementi della casella di posta archiviati possono essere ripristinati solo in posizione alternativa o su un disco locale. Inoltre, non è possibile ripristinare gli elementi standard della casella di posta in caselle di posta di archiviazione.

   Ripristina in posizione originale

   Consente di eseguire il ripristino dei messaggi di posta elettronica nella posizione originale di acquisizione dell'immagine di backup. I messaggi manterranno la stessa gerarchica e verranno ripristinati nella casella di posta e nella cartella originali.

   - Se il computer in uso non corrisponde al server attivo di Exchange, CA ARCserve D2D rileverà la posizione del server attivo su cui eseguire il ripristino dei messaggi di posta.
   - Se la casella di posta è stata spostata su un altro server Exchange della stessa organizzazione, CA ARCserve D2D rileverà il nuovo server Exchange su cui risiede la casella di posta originale ed eseguirà il ripristino su tale server.
   - Se il nome visualizzato per la casella di posta è stato modificato, qualsiasi tentativo di ripristino della casella di posta in posizione originale (da una precedente sessione di backup) non potrà essere completato, in quanto CA ARCserve D2D non sarà in grado di individuare il nome modificato. Per risolvere il problema, è possibile scegliere di ripristinare la casella di posta in una posizione alternativa.

Solo file di dettagli

Esegue il ripristino dei messaggi di posta elettronica su un disco. La posizione del disco deve corrispondere a un percorso locale. I messaggi ripristinati manterranno la stessa gerarchia della casella di posta di Exchange. Il nome del file viene utilizzato come oggetto del messaggio di posta elettronica.

Nota: se l'oggetto del messaggio di posta, il nome della cartella o il nome della casella di posta contengono i caratteri \/: *?, tali caratteri verranno sostituiti da un trattino (-) nel nome file. " < > |

Per risolvere una situazione di conflitto in un file system, sono disponibili due opzioni. Una stessa cartella non può contenere due file system, mentre ciò è possibile nel caso di messaggi di posta elettronica di Exchange.

- **Rinomina** - Se sul disco è presente un file con lo stesso nome dell'oggetto del messaggio di posta, CA ARCserve D2D aggiungerà un numero alla fine dell'oggetto del messaggio di posta.
- **Sovrascrivi** - Se sul disco è presente un file con lo stesso nome dell'oggetto del messaggio di posta, CA ARCserve D2D sovrascriverà il file.

Ripristina in posizione alternativa

Ripristina i messaggi in un percorso specificato o consente di individuare il percorso in cui ripristinare le immagini di backup. La destinazione deve essere una casella di posta facente parte della stessa organizzazione di Exchange. Sarà necessario specificare un nome per la nuova cartella. (Nei ripristini in posizione alternativa, la destinazione non può essere una cartella pubblica).

Dopo aver immesso il nome utente e la password, fare clic sul pulsante Sfoglia per visualizzare un elenco di tutti i server Exchange, dei gruppi di archiviazione, dei database di Exchange e delle caselle di posta presenti nell'organizzazione.

Selezionare una casella di posta come destinazione.

9. Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

10. Verificare che le opzioni di ripristino e le impostazioni siano corrette.

   - Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
   - Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

   Nota: se il processo di generazione catalogo e di ripristino granulare di Exchange è in esecuzione, la sessione di backup sarà in stato montato. Non eseguire alcuna operazione (formattazione, modifica della lettera di unità, eliminazione della partizione, ecc.) sul volume montato.

Visualizzazione dei registri CA ARCserve Central Protection Manager

Il registro attività contiene informazioni complete su tutte le operazioni eseguite dall'applicazione. Il registro fornisce l'itinerario di controllo di ciascun processo eseguito (le attività più recenti vengono elencate in prima posizione) e può essere utile per la risoluzione di eventuali problemi.

Per visualizzare i registri CA ARCserve Central Protection Manager

1. Dalla pagina principale, fare clic su Visualizza registri della barra di navigazione.

   Verrà visualizzata la schermata Visualizza registri.

2. Dagli elenchi a discesa, specificare le informazioni di registro che si desidera visualizzare.

   - **Gravità** - Consente di specificare la gravità del registro che si desidera visualizzare. È possibile specificare le seguenti opzioni di gravità:

     – **Tutto** - Consente di visualizzare tutti i registri indipendentemente dalla gravità.

     – **Informazioni** - Consente di visualizzare soltanto i registri che descrivono informazioni generali.

     – **Errori** - Consente di visualizzare soltanto i registri di descrizione di errori gravi.

     – **Avvisi** - Consente di visualizzare soltanto i registri di descrizione degli errori di avviso.

     – **Errori e avvisi** - Consente di visualizzare soltanto i registri di descrizione degli errori gravi e di avviso.

- **Modulo** - Consente di specificare il modulo di cui si desiderano visualizzare i registri. È possibile specificare le seguenti opzioni di modulo:
  - **Tutto** - Consente di visualizzare i registri relativi ai componenti delle applicazioni.
  - **Comune** - Consente di visualizzare i registri relativi ai processi comuni.
  - **Importa nodi dal rilevamento** - Consente di visualizzare i registri relativi ai nodi importati dal rilevamento.
  - **Importa nodi da hypervisor** - Consente di visualizzare i registri relativi ai nodi importati dall'hypervisor.
  - **Importa nodi da file** - Consente di visualizzare solo i registri relativi al processo di importazione dei nodi nell'applicazione a partire da un file.
  - **Gestione criterio** - Consente di visualizzare soltanto i registri relativi alla gestione dei criteri.
  - **Sincronizzazione di CA ARCserve Backup** - Consente di visualizzare soltanto i registri relativi alla sincronizzazione dei dati di CA ARCserve Backup.
  - **Sincronizzazione di CA ARCserve D2D** - Consente di visualizzare soltanto i registri relativi alla sincronizzazione dei dati di CA ARCserve D2D.
  - **Aggiornamenti per CA ARCserve D2D** - Consente di visualizzare soltanto i registri relativi alle modifiche apportate a CA ARCserve D2D.
  - **Aggiornamenti** - Consente di visualizzare soltanto i registri relativi all'aggiornamento dell'applicazione.
  - **Invia i processi di backup CA ARCserve D2D** - Consente di visualizzare soltanto i registri relativi a processi di backup CA ARCserve D2D inviati.
  - **Verifica preliminare** - Consente di visualizzare soltanto i registri relativi a operazioni di verifica preliminare.
  - **Invia processi di backup del computer virtuale** - Consente di visualizzare soltanto i registri relativi ai processi di backup del computer virtuale inviati.
- **Nome nodo** - Consente di visualizzare soltanto i registri relativi a un nodo specifico.

  Nota: questo campo supporta l'uso dei caratteri jolly '*' e '?'. Ad esempio, immettere 'lod*' per ripristinare tutti i registri attività per i computer il cui nome inizia per 'lod'.

Nota: è possibile applicare contemporaneamente le opzioni Gravità, Modulo e Nome nodo. Ad esempio, è possibile visualizzare Errori (Gravità) relativi agli Aggiornamenti (Modulo) per il Nodo X (Nome nodo).

Fare clic su Refresh (Aggiorna).

La visualizzazione dei registri dipende dalle opzioni di visualizzazione specificate.

Nota: l'ora visualizzata nel registro si basa sul fuso orario in cui risiede il server CA ARCserve Central Protection Manager.

Aggiungere collegamenti alla barra di spostamento

Per ogni applicazione CA ARCserve Central Applications è presente un collegamento Scheda Aggiungi nuovo sulla barra di navigazione. Questa funzionalità consente di aggiungere voci alla barra di navigazione per le ulteriori applicazioni Web che si desidera gestire. Tuttavia, per ciascuna applicazione installata, verrà aggiunto automaticamente un nuovo collegamento alla barra di navigazione. Ad esempio, se CA ARCserve Central Reporting e CA ARCserve Central Virtual Standby sono stati installati su un Computer A e CA ARCserve Central Reporting viene avviato, CA ARCserve Central Virtual Standby verrà aggiunto automaticamente alla barra di navigazione.

Nota: le applicazioni installate verranno rilevate soltanto se sono presenti altre istanze CA ARCserve Central Applications sullo stesso computer.

Procedere come descritto di seguito:

1. Dalla barra di navigazione dell'applicazione, fare clic sul collegamento Scheda Aggiungi nuovo.
2. Specificare il nome e l'URL per l'applicazione o il sito Web che si desidera aggiungere. Ad esempio, www.google.com.

   Facoltativamente, specificare il percorso di un'icona.
3. Fare clic su OK.

   La nuova scheda viene aggiunta nella parte inferiore della barra di navigazione.

Tenere presenti le seguenti considerazioni:

- Il collegamento al Supporto tecnico di CA viene aggiunto per impostazione predefinita.

Per rimuovere la nuova scheda, evidenziare la scheda e fare clic sul collegamento Rimuovi.

Procedura consigliata

Per l'applicazione CA ARCserve Central Protection Manager, tenere presenti le best practice seguenti:

- CA ARCserve Central Applications è in grado di recuperare dati per un nodo specifico da un computer remoto tramite le comunicazioni tra il computer locale CA ARCserve Central Applications e il computer remoto.

  Per garantire che l'accesso remoto funzioni correttamente, sono necessarie le seguenti restrizioni:

  - **Restrizione di rete** - L'amministratore remoto "admin$" deve essere abilitato sul computer remoto.
  - **Restrizione account utente** - Per accedere a CA ARCserve Central Applications, è necessario utilizzare l'account di amministratore dei bollettini dal computer locale di CA ARCserve Central Applications oppure rilasciare privilegi amministrativi al computer locale e al computer remoto di CA ARCserve Central Applications.

  Nota: per aggiungere un nodo, è necessario disporre dei privilegi di amministratore per il computer remoto.

- Per aggiungere nodi per nome nodo o indirizzo IP su un computer Windows Server 2008 R2, utilizzare l'account in base a uno dei seguenti requisiti:

  - Se si utilizza l'account del gruppo di amministratori dal computer CA ARCserve Central Applications e il computer remoto per accedere a CA ARCserve Central Applications, è possibile utilizzare lo stesso account per aggiungere un nodo.
  - Se si utilizza l'account Amministratore dei bollettini dal computer CA ARCserve Central Applications per accedere a CA ARCserve Central Applications, per aggiungere un nodo utilizzare l'account del gruppo di amministratori dal computer remoto.

- Per individuare i nodi da Active Directory, scegliere una delle opzioni seguenti:

  - Se si installa CA ARCserve Central Applications su un nodo che non è connesso a un dominio Windows, CA ARCserve Central Applications può avere accesso alle informazioni di Active Directory che risiedono sul controller di dominio.
  - Se si installa CA ARCserve Central Applications su un nodo collegato a un gruppo di lavoro, è necessario eseguire la seguente riga di comando nella finestra di comando per verificare che CA ARCserve Central Applications disponga dell'accesso al controller di dominio associato:

    ```
    nltest /dsgetdc:%domain_name%
    ```

    Nota: se questa opzione restituisce un errore con lo stato ERROR_NO_SUCH_DOMAIN (1355), sarà necessario modificare le impostazioni di rete.

Modifica del protocollo di comunicazione del server

Per impostazione predefinita, CA ARCserve Central Applications utilizza il protocollo HTTP (Hypertext Transfer Protocol) per la comunicazione tra i componenti. Se si desidera utilizzare un livello di protezione superiore per la comunicazione delle password tra i componenti, è possibile utilizzare il protocollo HTTPS (Hypertext Transfer Protocol Secure). Se non si desidera utilizzare tale livello di protezione aggiuntivo, è possibile modificare il protocollo utilizzato selezionando HTTP.

Procedere come descritto di seguito:

1. Accedere al computer di installazione dell'applicazione utilizzando un account amministrativo o un account con privilegi di amministratore.

   Nota: se l'accesso non viene eseguito con un account amministrativo o un con privilegi di amministratore, sarà necessario configurare la riga di comando per l'esecuzione con privilegi di amministratore.

2. Aprire la riga di comando di Windows.

3. Eseguire una delle seguenti operazioni:

   - **Per modificare il protocollo da HTTP a HTTPS:**

     Avviare l'utilità "changeToHttps.bat" dal percorso predefinito riportato di seguito (la posizione della cartella BIN può variare in base al percorso di installazione dell'applicazione):

     `C:\Programmi\CA\ARCserve Central Applications\BIN`

     Una volta apportate le modifiche al protocollo, verrà visualizzato il messaggio seguente:

     `Il protocollo di comunicazione è stato convertito in HTTPS.`

   - **Per modificare il protocollo da HTTPS a HTTP:**

     Avviare l'utilità "changeToHttp.bat" dal percorso predefinito riportato di seguito (la posizione della cartella BIN può variare in base al percorso di installazione dell'applicazione):

     `C:\Programmi\CA\ARCserve Central Applications\BIN`

     Una volta apportate le modifiche al protocollo, verrà visualizzato il messaggio seguente:

     `Il protocollo di comunicazione è stato convertito in HTTP.`

4. Riavviare il browser e connettersi nuovamente a CA ARCserve Central Applications.

   Nota: in caso di modifica del protocollo in HTTPS, verrà visualizzato un avviso nel browser Web. Questo comportamento è causato da un certificato di protezione autofirmato che richiede all'utente di ignorare l'avviso e continuare oppure di aggiungere il certificato al browser per evitarne la visualizzazione.

Capitolo 5: Integrazione di CA ARCserve Central Protection Manager con gli strumenti del server di gestione IT

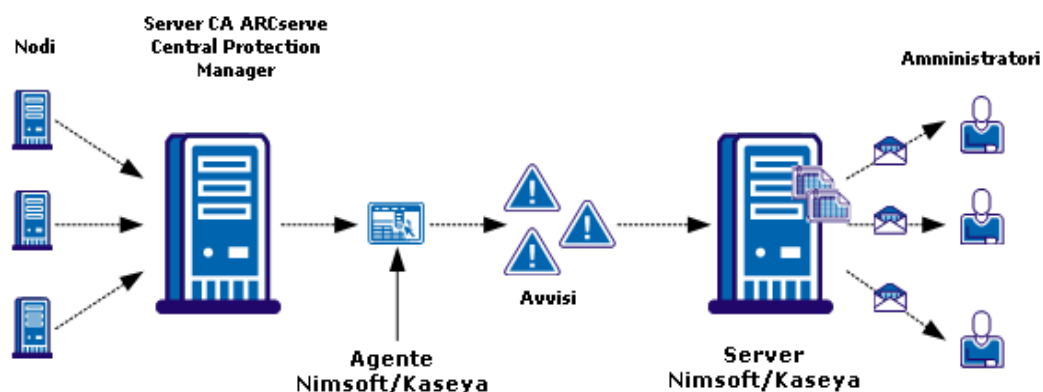
Questa sezione contiene i seguenti argomenti:

Modalità di integrazione di CA ARCserve Central Protection Managercon Nimsoft e Kaseya

È possibile configurare CA ARCserve Central Protection Manager per la pubblicazione in tempo reale delle informazioni relative ai messaggi di avviso negli strumenti di gestione dell'infrastruttura del server di gestione IT. Questa funzionalità consente agli amministratori della gestione IT del server di rispondere agli avvisi di CA ARCserve Central Protection Manager in modo efficace.

CA ARCserve Central Protection Manager viene integrato con gli strumenti di gestione dell'infrastruttura del server di gestione IT riportati di seguito:

- Nimsoft
  - Server: 5.11
  - Robot: 5.32
  - UMP: 2.1.2
- Kaseya
  - Server: 6.1.0.0
  - Agente: 6.1.0.6

La modalità di integrazione di CA ARCserve Central Protection Manager con Nimsoft e Kaseya è illustrata nel diagramma seguente:

Il server CA ARCserve Central Protection Manager esegue il monitoraggio dei nodi sui cui è stato CA ARCserve D2D. Quando il server CA ARCserve Central Protection Manager individua una condizione di avviso, invia gli avvisi all'agente Nimsoft o Kaseya installato sul server CA ARCserve Central Protection Manager. L'agente inoltra immediatamente gli avvisi al server Nimsoft o Kaseya.

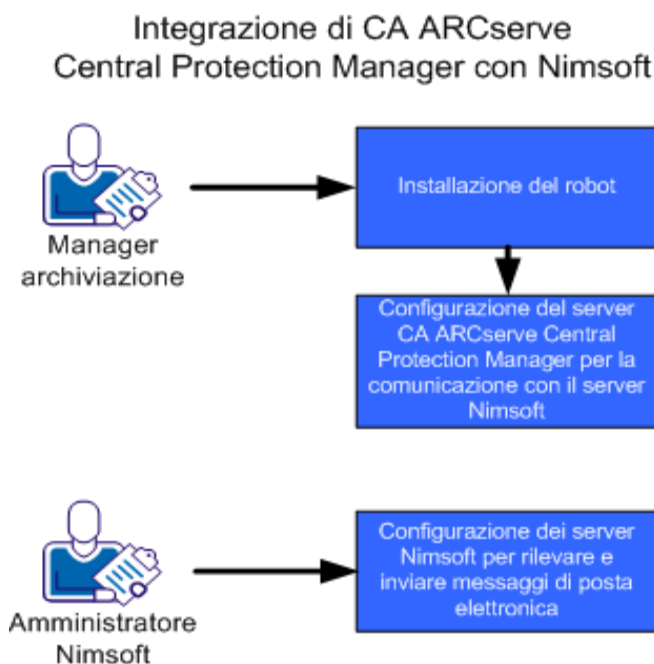
CA ARCserve Central Protection Manager esegue il monitoraggio degli avvisi generati dalle applicazioni seguenti:

- CA ARCserve D2D
- CA ARCserve Central Virtual Standby
- CA ARCserve Central Host-Based VM Backup
- CA ARCserve Central Protection Manager

Il server Nimsoft o Kaseya genera rapporti sui nodi di esecuzione di tali applicazioni che possono essere visualizzate dagli amministratori mediante gli strumenti di gestione Nimsoft e Kaseya. È possibile configurare i server Nimsoft e Kaseya per l'invio di messaggi di posta elettronica agli amministratori, in base a criteri predefiniti.

Modalità di integrazione di CA ARCserve Central Protection Manager con Nimsoft

I manager dell'archiviazione possono configurare CA ARCserve Central Protection Manager per la comunicazione dei messaggi di avviso ai server Nimsoft. Gli amministratori Nimsoft possono configurare gli strumenti di gestione dell'infrastruttura IT di Nimsoft per rilevare gli avvisi di CA ARCserve Central Protection Manager, generare rapporti sugli avvisi e inviare messaggi di posta elettronica. Gli amministratori possono utilizzare tali rapporti per gestire lo stato dei nodi di CA ARCserve D2D.

Il diagramma seguente mostra la procedura che deve essere eseguita dai manager dell'archiviazione per l'integrazione di CA ARCserve Central Protection Manager con gli strumenti di gestione dell'infrastruttura IT di Nimsoft:

Per eseguire l'integrazione di CA ARCserve Central Protection Manager con Nimsoft, attenersi alla procedura seguente:

1. Installare il robot (a pagina 172).
2. Configurare il server CA ARCserve Central Protection Manager per la comunicazione con il server Nimsoft (a pagina 174).
3. Configurare il server Nimsoft per il rilevamento e l'invio dei messaggi di posta elettronica (a pagina 174).

Nota: quando i server CA ARCserve Central Protection Manager inviano messaggi di avviso contenenti caratteri localizzati ai server Nimsoft, tali caratteri possono essere visualizzati come testo confuso nella console di allarme di Nimsoft Unified Monitoring Portal (UMP). Per evitare questo comportamento, configurare il server Nimsoft per l'utilizzo della codifica UTF-8. Per ulteriori informazioni, consultare il paragrafo Characters from Localized Servers Appear as Garbled Text in the Nimsoft UMP Alarm Console nella Guida per l'utente di CA ARCserve Central Protection Manager.

Installazione del robot

L'installazione del robot viene eseguita sul server CA ARCserve Central Protection Manager. Il robot consente al server CA ARCserve Central Protection Manager di comunicare e inviare in tempo reale i messaggi di avviso al server Nimsoft.

Nota: prima di eseguire il programma di installazione, verificare di disporre di una licenza valida.

Procedere come descritto di seguito:

1. Scaricare o copiare il file di installazione del robot sul computer.

   Fare doppio clic su *NimBUS Robot.exe* per avviare l'installazione.

   Viene visualizzata la finestra di dialogo Contratto di licenza.

2. Nella finestra di dialogo della licenza, fare clic su Sì per avviare l'installazione.

   Verrà visualizzata la finestra di dialogo per la selezione della destinazione di installazione.

3. Specificare la posizione desiderata per l'installazione del robot oppure are clic su Next (Avanti) per accettare la directory predefinita.

   Verrà visualizzata la finestra di dialogo di selezione del sistema operativo.

4. Selezionare Normal Installation (Installazione normale) e fare clic su Next (Avanti).

   Viene visualizzata la finestra di dialogo Nimsoft Domain (Dominio Nimsoft) contenente un elenco dei domini rilevati.

5. Selezionare la casella di controllo accanto all'opzione Choose to connect to the network interface through IP address (Connessione all'interfaccia di rete mediante indirizzo IP) e fare clic su Next (Avanti).

   Verrà visualizzata la finestra di dialogo Specify Nimsoft Hub IP Address (Specificare un indirizzo IP per l'hub Nimsoft).

6. Nel campo Hub IP (IP hub), specificare l'indirizzo IP dell'hub Nimsoft desiderato per l'invio dei messaggi di avviso da parte del server CA ARCserve Central Protection Manager.

   Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Options (Opzioni).

7. Completare i campi seguenti nella finestra di dialogo Options (Opzioni):

   (Facoltativo) First probe port (Prima porta di esplorazione)

   Consente di specificare il numero della prima porta da utilizzare all'avvio dell'esplorazione.

   Nota: non specificare la porta per consentire al sistema operativo di utilizzare le porte in modo casuale.

   Passive mode (Modalità passiva)

   Specificare questa modalità solo se il robot non è in grado di comunicare con l'hub Nimsoft. Se l'hub Nimsoft è in grado di comunicare con il server CA ARCserve Central Protection Manager, fare clic sulla casella di controllo accanto a Passive mode (Modalità Passiva).

   Nota: se si specifica questa opzione, aggiungere manualmente il robot passivo alla configurazione dell'hub.

   Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Start Copying Files (Avvia copia dei file).

8. Fare clic su Avanti.

   Il programma procede all'installazione del robot.

9. Una volta completata l'installazione, fare clic su Finish (Fine).

L'installazione del robot verrà completata.

Configurazione del server CA ARCserve Central Protection Manager per la comunicazione con il server Nimsoft

CA ARCserve Central Protection Manager consente di inviare messaggi di avviso ai server di gestione IT Nimsoft. Per inviare le informazioni di avviso, configurare il server CA ARCserve Central Protection Manager per la comunicazione con il server Nimsoft.

Procedere come descritto di seguito:

1. Accedere a CA ARCserve Central Protection Manager e fare clic su Configurazione nella barra di navigazione.

   Verranno visualizzate le opzioni di configurazione.

2. Fare clic su Configurazione del server di gestione IT dall'elenco Configurazione.

   Verranno visualizzate le opzioni di configurazione del server di gestione IT.

3. Completare le seguenti operazioni:

   a. Fare clic su Abilita.

   b. Fare clic su Nimsoft.

   c. Specificare un metodo di ripetizione. Il metodo di ripetizione definisce i giorni della settimana per il rinvio delle notifiche di avviso al server Nimsoft in caso di errore del processo di invio originale. Tale errore può verificarsi nel caso in cui il server Nimsoft non sia in linea o non sia disponibile.

   d. Specificare una pianificazione. L'opzione Pianifica definisce l'orario di rinvio delle notifiche di avviso al server Nimsoft.

   Fare clic su Salva.

La configurazione del server CA ARCserve Central Protection Manager per la comunicazione con il server Nimsoft viene completata.

Configurazione del server Nimsoft per il rilevamento e l'invio dei messaggi di posta elettronica

Gli amministratori Nimsoft possono configurare la console secondaria di allarme per l'invio dei messaggi di posta elettronica ai destinatari specificati, in caso di rilevamento di messaggi di avviso dei server CA ARCserve Central Protection Manager. Per ulteriori informazioni, consultare la documentazione di Nimsoft.

Visualizzazione delle informazioni relative agli avvisi nella console secondaria Nimsoft.

La console secondaria di allarme Nimsoft consente agli amministratori Nimsoft di visualizzare le informazioni relative agli avvisi CA ARCserve Central Protection Manager. La console secondaria di allarme Nimsoft fornisce le seguenti informazioni sugli avvisi CA ARCserve Central Protection Manager:

Host Name (Nome host)

Specifica il nome host del server CA ARCserve Central Protection Manager che ha inviato l'avviso al server Nimsoft.

Source (Origine)

Specifica l'indirizzo IP del server CA ARCserve Central Protection Manager che ha inviato l'avviso al server Nimsoft.

Severity (Gravità)

Specifica la gravità dell'avviso inviato al server Nimsoft.

Subsystem (Sottosistema)

Specifica il nome host del server che ha rilevato la condizione di avviso.

Esempio: la condizione di avviso si verifica su un server CA ARCserve D2D. Il campo di sistema specifica il nome host del server CA ARCserve D2D.

Subsystem ID (ID sottosistema)

Specifica l'indirizzo IP del server che ha rilevato la condizione di avviso.

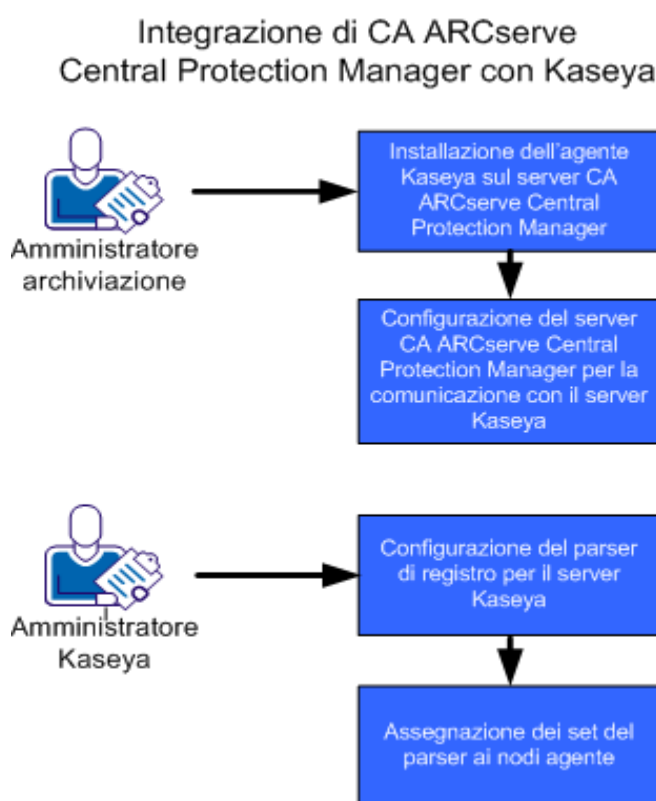
La console secondaria di allarme consente agli amministratori Nimsoft di eseguire diverse attività:

- Configurare la console secondaria di allarme per l'invio dei messaggi di posta elettronica ai destinatari specificati in caso di rilevamento di avvisi
- Visualizzare la cronologia degli avvisi
- Confermare gli avvisi
- Assegnare gli avvisi ai tecnici

Nota: per ulteriori informazioni sull'uso della console secondaria di allarme Nimsoft, consultare la documentazione di Nimsoft.

Modalità di integrazione di CA ARCserve Central Protection Manager con Kaseya

I manager dell'archiviazione possono configurare CA ARCserve Central Protection Manager per la comunicazione dei messaggi di avviso ai server Kaseya. Gli amministratori Kaseya possono configurare gli strumenti di gestione dell'infrastruttura IT di Kaseya per rilevare gli avvisi di CA ARCserve Central Protection Manager, generare rapporti sugli avvisi e inviare messaggi di posta elettronica. Gli amministratori possono utilizzare tali rapporti per gestire lo stato dei nodi di CA ARCserve D2D.

Il diagramma seguente mostra la procedura che deve essere eseguita dai manager di backup per l'integrazione di CA ARCserve Central Protection Manager con gli strumenti di gestione dell'infrastruttura IT di Kaseya:

Per eseguire l'integrazione di CA ARCserve Central Protection Manager con Kaseya, attenersi alla procedura seguente:

1. Installare l'agente Kaseya sul server CA AR (a pagina 177)Cserve Central Protection Manager.
2. Configurare il server CA ARCserve Central Protection Manager per la comunicazione con il server Kaseya (a pagina 178).

3. Configurare il parser di registro per il server Kaseya (a pagina 178).
4. Assegnare il set di parser sui nodi dell'agente (a pagina 181).

Installazione dell'agente Kaseya

Installare l'agente Kaseya sul server CA ARCserve Central Protection Manager per consentirne la comunicazione con il server Kaseya. Per installazione, eseguire la distribuzione dell'agente dalla console di gestione IT Kaseya.

Procedere come descritto di seguito:

1. Aprire una finestra del browser ed eseguire l'accesso alla console di gestione IT Kaseya.

   Dalla barra di navigazione presente sul lato sinistro della finestra, fare clic su Agent (Agente).

   Verranno visualizzate le opzioni dell'agente.

2. Espandere Install Agents (Installazione agenti) e fare clic su Deploy Agents (Distribuisci agenti).

   Verranno visualizzate le opzioni di distribuzione degli agenti.

3. Selezionare una delle seguenti opzioni:

   Click to download default Agent (Fare clic per eseguire il download dell'agente predefinito)

   Consente di eseguire il download e salvare il file di installazione sul computer di destinazione.

   Una volta completato il download, eseguire i file di installazione dell'agente direttamente dal computer di destinazione.

   Create Package (Crea pacchetto)

   Consente di creare un'utilità di installazione pacchetti per eseguire l'installazione dell'agente su uno o più computer. Seguire le istruzioni visualizzate sullo schermo per creare un pacchetto di installazione. Per ulteriori informazioni, consultare la documentazione di Kaseya.

L'installazione dell'agente viene completata.

Configurazione del server CA ARCserve Central Protection Manager per la comunicazione con il server Kaseya.

CA ARCserve Central Protection Manager consente di inviare messaggi di avviso ai server di gestione IT Kaseya. Per inviare le informazioni di avviso, configurare il server CA ARCserve Central Protection Manager per la comunicazione con il server Kaseya.

Procedere come descritto di seguito:

1. Accedere a CA ARCserve Central Protection Manager e fare clic su Configurazione nella barra di navigazione.

   Verranno visualizzate le opzioni di configurazione.

2. Fare clic su Configurazione del server di gestione IT dall'elenco Configurazione.

   Verranno visualizzate le opzioni di configurazione del server di gestione IT.

3. Completare le seguenti operazioni:

   a. Fare clic su Abilita.

   b. Fare clic su Kaseya.

   c. Specificare un metodo di ripetizione. Il metodo di ripetizione definisce i giorni della settimana per il rinvio delle notifiche di avviso al server Kaseya in caso di errore del processo di invio originale. Tale errore può verificarsi nel caso in cui il server Kaseya non sia in linea o non sia disponibile.

   d. Specificare una pianificazione. L'opzione Pianifica definisce l'orario di rinvio delle notifiche di avviso al server Kaseya.

   Fare clic su Salva.

La configurazione del server CA ARCserve Central Protection Manager per la comunicazione con il server Kaseya viene completata.

Configurazione del parser di registro per il server Kaseya.

Per visualizzare le informazioni relative agli avvisi di CA ARCserve Central Protection Manager, configurare il server Kaseya per la lettura dei dati nei file di registro degli avvisi di CA ARCserve Central Protection Manager.

Procedere come descritto di seguito:

1. Aprire una finestra del browser ed eseguire l'accesso alla console di gestione IT Kaseya.

2. Dalla barra di navigazione presente sul lato sinistro della finestra, fare clic su Monitor.

   Vengono visualizzate le opzioni di monitoraggio.

3. Espandere Log Monitoring (Monitoraggio registro) e fare clic su Log Parser (Parser di registro).

   Verranno visualizzate le opzioni di configurazione del parser del registro.

4. Nell'elenco Machine.Group ID, fare clic sulla casella di controllo accanto al serve CA ARCserve Central Protection Manager.

   Dall'elenco a discesa Log File Parser (Parser file di registro) fare clic su <Select Log Parser> (Seleziona parser di registro).

   Fare clic su New (Nuovo).

   Verrà visualizzata la finestra di dialogo Log File Parser Definition (Definizione del parser file di registro).

5. Completare i campi seguenti della finestra di dialogo Log File Parser Definition (Definizione del parser file di registro):

   Parser Name (Nome parser)

   Definisce il nome del file parser dei file di registro.

   Log File Path (Percorso file di registro)

   Definisce il percorso del file di registro sul server CA ARCserve Central Protection Manager. Il percorso per il file di registro è il seguente:

   ```
   <HOME_CA ARCserve Central Applications>\ITMgmtIntegration\<log_fle_name>
   ```

   CA ARCserve Central Protection Manager genera il file di registro per il supporto dei caratteri Unicode e non Unicode. I nomi dei file registro sono i seguenti:

   Non Unicode:

   `CentralAppAlertsForKaseyaANSI.log`

   Unicode:

   `CentralAppAlertsForKaseyaUTF8.log`

   Importante. La console di gestione IT Kaseya non supporta i caratteri Unicode. Pertanto, utilizzare i file di registro denominati CentralAppAlertsForKaseyaANSI.log.

Log Archive Path (Percorso archivio di registro)

Definisce il percorso del file di registro archiviato sul server CA ARCserve Central Protection Manager. Per impostazione predefinita, Protection Manager esegue l'archiviazione dei file di registro con dimensioni superiori ai 10 MBYTE.

Nota: per specificare un valore di archiviazione diverso dei file di registro per Protection Manager, modificare il valore (in MB)MaxLogFileSize nel file seguente:

```
<HOME_CA ARCserve Central Applications>\ITMgmtIntegration\Configuration\E
dge-ITMgmtIntegration.INI
```

Descrizione

Fornisce una descrizione del file parser dei file di registro.

Template (Modello)

Definisce il formato dei dati contenuti nei file di registro sul server CA ARCserve Central Protection Manager. Utilizzare la seguente sintassi:

```
$CACentral Protection Manager Machine Name$ [$Alert Generated Product$]
$Alert Generated Machine Name$ $Severity$ $Send Time From Origin Product$
$Alert Message$
```

Output Template (Modello di output)

Definisce il formato dei dati di output per il server Kaseya. Utilizzare la seguente sintassi:

```
$Protection Manager Server$ $Generated by$ $Host Name$ $Severity$ $Sent$
$Message$
```

Log File Parameters (Parametri del file di registro)

Creare i seguenti parametri del file di registro:

Nota: specificare il tipo di parametro e fare clic su Apply (Applica) per salvare il parametro.

Nome computer CA ARCserve Central Protection Manager

Tipo: String

Prodotto dell'avviso generato

Tipo: String

Nome computer dell'avviso generato

Tipo: String

Severity (Gravità)

Tipo: String

Ora di invio dal prodotto di origine

Tipo: DateTime

Formato: YYYY-MM-DD hh:mm:ss

Messaggio di avviso

Tipo: String

Fare clic su Salva.

La definizione del parser di registro viene salvata.

6. Fare clic su Chiudi.

La finestra di dialogo Log Parser Definition viene chiusa e il file di definizione del parser di registro viene creato e applicato al server CA ARCserve Central Protection Manager.

Assegnazione dei set del parser sul server Kaseya

Configurare i set del parser per filtrare le informazioni relative agli avvisi di CA ARCserve Central Protection Manager nella console di gestione Kaseya. I set del parser definiscono le condizioni da filtrare. Ad esempio, è possibile filtrare gli avvisi in base al livello di gravità, agli errori di backup, ecc.

Procedere come descritto di seguito:

1. Aprire una finestra del browser ed eseguire l'accesso alla console di gestione IT Kaseya.
2. Dalla barra di navigazione presente sul lato sinistro della finestra, fare clic su Monitor.

   Vengono visualizzate le opzioni di monitoraggio.

3. Espandere Log Monitoring e fare clic su Assign Log Parser.

   Verranno visualizzate le opzioni dei set di parser del registro

4. Nella sezione Assign log parser sets to selected machines (Assegna set di parser del registro ai computer selezionati) specificare le opzioni di avviso desiderate.

5. Dall'elenco a discesa Select log parser (Selezionare parser di registro), fare clic sul parser di registro che si desidera assegnare ai set di parser.

   Dall'elenco a discesa Define parser (Definisci set di parser), fare clic su <New Parser Set> (Nuovo set di parser).

   Verrà visualizzata la finestra di dialogo Edit Parser Set (Modifica set di parser).

6. Nel campo Parser Set Name (Nome set di parser), specificare il nome desiderato per il set e fare clic su New (Nuovo).

   Verranno visualizzate le opzioni di analisi.

7. Specificare i seguenti valori:

   Parser Column (Colonna parser)

   Definisce il parametro da filtrare.

   Operator (Operatore)

   Definisce la modalità di filtro dei dati contenuti nel parametro.

   Parameter File (File dei parametri)

   Definisce il valore del parametro da filtrare.

   Far clic su Add (Aggiungi) e quindi su Close (Chiudi).

   Il filtro viene applicato al set di parser e la finestra di dialogo Edit Parser Set (Modifica set di parser) viene chiusa.

   Nota: il paragrafo Esempi di filtri dei set di parser contiene esempi riguardanti la definizione dei filtri del set di parser.

8. Dall'elenco a discesa Select log parser (Selezionare parser di registro), fare clic sul parser di registro che si desidera applicare.

   Dall'elenco a discesa Define parser sets (Definisci set di parser), selezionare il set di parser creato.

   Dalla colonna Machine IDs (ID computer), fare clic sulla casella di controllo accanto ai server desiderati per l'applicazione del set di parser.

   Fare clic su Apply (Applica).

Il parser di registro e il set di parser vengono assegnati.

Esempi di filtri dei set di parser

Per creare set di parser che consentano di filtrare solamente gli avvisi con errori, specificare i valori seguenti:

Parser Column (Colonna parser)

Severity (Gravità)

Operator (Operatore)

Equal

Filtro di parametro

errore

Per creare set di parser per la visualizzazione di tutti gli avvisi, indipendentemente dal livello di gravità, specificano i valori seguenti:

Parser Column (Colonna parser)

Severity (Gravità)

Operator (Operatore)

Contains

Filtro di parametro

error, warning, information

Per creare set di parser per la sola visualizzazione degli avvisi di backup non riuscito, specificare i valori seguenti:

Parser Column (Colonna parser)

Messaggio di avviso

Operator (Operatore)

Contains

Filtro di parametro

backup, failed

Configurazione dei server Kaseya per il rilevamento e l'invio dei messaggi di posta elettronica.

Gli amministratori Kaseya possono configurare la console secondaria di allarme per l'invio dei messaggi di posta elettronica ai destinatari specificati, in caso di rilevamento di messaggi di avviso dei server CA ARCserve Central Protection Manager. Per ulteriori informazioni, consultare la documentazione di Kaseya.

Visualizzazione delle informazioni relative agli avvisi nel sistema di monitoraggio del registro dell'agente Kaseya

Il monitoraggio del registro dell'agente Kaseya consente di visualizzare i registri di avviso in base ai criteri definiti nel parser di registro e nel set di parser. I registri consentono di identificare ed eseguire azioni correttive per la condizione di avviso.

Per visualizzare le informazioni relative agli avvisi nel sistema di monitoraggio del registro dell'agente Kaseya:

1. Aprire una finestra del browser ed eseguire l'accesso alla console di gestione IT Kaseya.

   Dalla barra di navigazione presente sul lato sinistro della finestra, fare clic su Agent (Agente).

   Verranno visualizzate le opzioni dell'agente.

2. Espandere Machine Status (Stato computer) e fare clic su Agent Logs (Registri dell'agente).

   I registri dell'agente vengono visualizzati nel lato destro della finestra.

3. Dall'elenco dei server, fare clic sul server desiderato per visualizzare le informazioni corrispondenti.

   Fare clic su Refresh (Aggiorna).

Verranno visualizzate le informazioni relative ai messaggi di avviso per il server specificato.

Capitolo 6: Risoluzione dei problemi relativi a CA ARCserve Central Protection Manager

In questa sezione vengono fornite informazioni che consentono di identificare e risolvere i problemi che possono verificarsi durante l'utilizzo di CA ARCserve Central Protection Manager.

Questa sezione contiene i seguenti argomenti:

Messaggi di errore di connessione al server specificato durante il tentativo di aggiunta dei nodi.

Valido per piattaforme Windows.

Sintomo:

Quando si tenta di aggiungere o di stabilire la connessione a nodi dalla schermata Nodo, viene visualizzato il seguente messaggio di errore.

```
Impossibile connettersi al server specificato.
```

Soluzione:

Se tale messaggio viene visualizzato quando si tenta di aggiungere nodi dalla schermata Nodo, le seguenti azioni correttive possono contribuire alla risoluzione del problema:

- Verificare che il servizio Windows Server sia in esecuzione sul server CA ARCserve Central Protection Manager e sul computer virtuale (nodo) di origine.
- Assicurarsi che sia applicata un'eccezione di Windows Firewall al servizio Condivisione file e stampanti di Windows sul server CA ARCserve Central Protection Manager e sul computer virtuale (nodo) di origine.
- Assicurarsi che un'eccezione di Windows Firewall sia applicata al servizio Netlogon di Windows solo se il nodo non è membro di un dominio. Eseguire questa attività sul server CA ARCserve Central Protection Manager sul computer virtuale (nodo) di origine.
- Verificare che il valore applicato al modello Condivisione e protezione per l'account locale sia Classico. Per applicare il valore Classico, procedere come segue:

  Nota: eseguire i seguenti passaggi sul server CA ARCserve Central Protection Manager e sul computer virtuale (nodo) di origine.

  1. Accedere al server CA ARCserve Central Protection Manager e aprire il Pannello di controllo.
  2. Dal Pannello di controllo selezionare Strumenti di amministrazione.
  3. Fare doppio clic su Criteri di protezione locali.

     Verrà visualizzata la finestra di dialogo Criteri di protezione locali.

4. Dalla finestra Criteri di protezione locali, espandere Criteri locali e Opzioni di protezione.

   Verranno visualizzati i criteri di protezione.

5. Fare clic con il pulsante destro del mouse su Accesso alla rete: modello di condivisione e protezione per gli account locali e scegliere Proprietà dal menu di scelta rapida.

   Verrà visualizzata la finestra delle proprietà Accesso alla rete: modello di condivisione e protezione per gli account locali.

6. Fare clic su Impostazioni di protezione locali.

   Dall'elenco a discesa, selezionare Classico: gli utenti locali effettuano l'autenticazione di se stessi.

   Fare clic su OK.

- Verificare che il valore applicato ai criteri locali per il livello di autenticazione del manager della rete LAN sia impostato su invia LM & NTLMv2 – utilizza la protezione di sessione NTLMv2 se negoziata. Per applicare il valore, eseguire le seguenti operazioni:

  1. Accedere al server CA ARCserve Central Protection Manager e aprire il prompt dei comandi.

     Eseguire il seguente comando

     ```
     secpol.msc
     ```

     Verrà visualizzata la finestra di dialogo Impostazioni protezione locale.

  2. Selezionare i criteri locali e fare clic sulle opzioni di protezione.

     Ricerca di protezione di rete: livello di autenticazione di manager rete LAN.

     Fare doppio clic sull'opzione.

     Verrà visualizzata la finestra di dialogo Proprietà.

  3. Selezionare l'opzione seguente e fare clic su OK.

     ```
     invia LM & NTLMv2 – utilizza la protezione di sessione NTLMv2 se
     negoziata.
     ```

  4. Dal prompt dei comandi, eseguire il comando riportato di seguito:

     ```
     gpupdate
     ```

  Il valore viene applicato.

Pagine Web vuote o errori Javascript.

Valido sui sistemi operativi Windows Server 2008 e Windows Server 2003.

Sintomo:

Quando i siti Web di CA ARCserve Central Applications vengono aperti utilizzando Internet Explorer, vengono visualizzate pagine Web vuote oppure si verificano errori Javascript. Il problema si verifica quando si apre Internet Explorer sui sistemi operativi Windows Server 2008 e Windows Server 2003.

Questo problema si verifica nei seguenti casi:

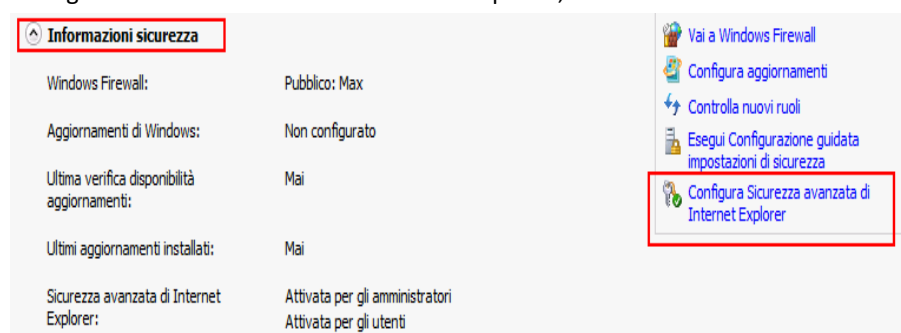
- Quando si utilizza Internet Explorer 8 o Internet Explorer 9 per visualizzare l'applicazione e il browser non riconosce l'URL come sito attendibile.
- Quando si utilizza Internet Explorer 9 per visualizzare l'applicazione e il protocollo di comunicazione in uso è HTTPS.

Soluzione:

Per risolvere il problema, disattivare la protezione avanzata di Internet Explorer sui computer utilizzati per visualizzare l'applicazione.

Per disattivare la protezione avanzata di Internet Explorer su sistemi Windows Server 2008, procedere come segue:

1. Accedere al computer Windows Server 2008 utilizzato per visualizzare i rapporti utilizzando l'account di amministratore o un account che dispone di privilegi amministrativi.
2. Fare clic con il pulsante destro su Computer sul desktop e scegliere Gestisci per aprire la finestra di Server Manager.
3. Dalla finestra Server manager fare clic su Server Manager (nome server).

   Dalla sezione Riepilogo server, aprire Informazioni di protezione e fare clic su Configura Protezione avanzata di Internet Explorer, come illustrato a continuazione:

   Viene visualizzata la finestra di dialogo Protezione avanzata di Internet Explorer.

4. Nella finestra di dialogo Protezione avanzata di Internet Explorer, procedere come segue:

   - Disattiva il controllo Administrators--Click
   - Disattiva il controllo Users--Click

   Fare clic su OK.

La finestra di dialogo Protezione avanzata di Internet Explorer viene chiusa e la protezione di Internet Explorer viene disabilitata.

Per disattivare la protezione avanzata di Internet Explorer su sistemi Windows Server 2003, procedere come segue:

1. Accedere al computer Windows Server 2003 utilizzato per visualizzare i rapporti utilizzando l'account di amministratore o un account che dispone di privilegi amministrativi.
2. Aprire il Pannello di controllo di Windows, quindi aprire Installazione applicazioni.
3. Dalla finestra di dialogo Installazione applicazioni selezionare l'opzione Installazione componenti di Windows per avviare l'Aggiunta guidata componenti di Windows.

   Eliminare il segno di spunta accanto a Protezione avanzata di Internet Explorer.

   Fare clic su Avanti.

   Proseguire seguendo le istruzioni visualizzate per completare l'installazione, quindi fare clic su Fine.

La protezione avanzata di Internet Explorer è disabilitata.

Le pagine Web non vengono caricate correttamente quando si accede ai nodi CA ARCserve D2D

Valido per piattaforme Windows.

Sintomo:

Le pagine Web non vengono caricate correttamente nel browser e/o vengono visualizzati messaggi di errore quando si accede ai nodi CA ARCserve D2D dalla schermata Nodi.

Soluzione:

Questo comportamento interessa principalmente i browser Internet Explorer. È possibile che le pagine Web non vengano caricate correttamente quando l'esecuzione script, i controlli ActiveX o i programmi Java sono disabilitati nel computer o bloccati sulla rete.

Per risolvere il problema, aggiornare la finestra del browser. Se il problema persiste dopo l'aggiornamento della finestra del browser, procedere come segue:

1. Aprire Internet Explorer.

   Scegliere Opzioni Internet dal menu Strumenti.

   Verrà visualizzata la finestra di dialogo Opzioni Internet.

2. Fare clic sulla scheda Protezione.

   Vengono visualizzate le opzioni di sicurezza.

3. Fare clic sull'area Internet.

   Vengono visualizzate le opzioni relative all'area Internet.

4. Fare clic su Livello personalizzato.

   Viene visualizzata la finestra di dialogo Impostazioni di sicurezza - Area Internet.

5. Scorrere fino alla categoria Esecuzione script.

   individuare Esecuzione script attivo.

   Selezionare l'opzione Attiva o Chiedi conferma.

6. Fare clic su OK nella finestra di dialogo impostazioni di sicurezza - Area Internet.

   La finestra di dialogo Impostazioni di sicurezza - Area Internet viene chiusa.

7. Fare clic su OK nella finestra di dialogo Opzioni Internet.

   La finestra di dialogo Opzioni Internet viene chiusa e l'opzione di esecuzione script attivo viene applicata.

Nota: se il problema non viene risolto, contattare l'amministratore di sistema per verificare che altri programmi, ad esempio programmi antivirus o firewall, non blocchino l'esecuzione degli script attivi, i controlli ActiveX o i programmi Java.

Viene visualizzato un messaggio relativo a credenziali non valide durante l'aggiunta di nodi

Valido per piattaforme Windows.

Sintomo:

Quando si tenta di aggiungere nodi alla schermata Nodi, viene visualizzato il seguente messaggio:

```
Credenziali non valide.
```

Soluzione:

Questo problema si verifica nei seguenti casi:

- Le credenziali specificate nella finestra di dialogo Aggiungi nodi non sono corrette.
- L'orario sul nodo non corrisponde all'orario sul server applicazioni.

Per risolvere il problema, procedere come segue:

1. Accedere al server applicazioni e quindi accedere all'applicazione.
2. Dalla pagina principale, selezionare Nodo nella barra di navigazione.

   Verrà visualizzata la schermata Nodo.

3. Dalla barra degli strumenti Nodo, fare clic su clic Aggiungi, quindi selezionare Aggiungi nodo per IP/Nome dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Aggiungi nodo per IP/Nome.

4. Completare i seguenti campi:
   - **IP/Nome nodo** - Consente di specificare l'indirizzo IP o il nome del nodo.
   - **Descrizione** - Consente di specificare una descrizione per il nodo.
   - **Nome utente** - Consente di specificare il nome utente richiesto per l'accesso al nodo.
   - **Password** - Consente di specificare la password richiesta per l'accesso al nodo.

Fare clic su Convalida.

5. Se viene visualizzato il messaggio Credenziali non valide, procedere come segue:

   a. Verificare di avere specificato le credenziali corrette nella finestra di dialogo Aggiungi nodi e quindi fare clic su Convalida.

   b. Se viene visualizzato il messaggio Credenziali non valide, assicurarsi che l'orario del sistema operativo del server applicazioni corrisponda all'orario del sistema operativo sul nodo.

      Nota: gli orari dei sistemi operativi possono appartenere a diversi fusi orari. Le date dei sistemi operativi, tuttavia, non possono essere diverse. In particolare, assicurarsi che la data del sistema operativo sul nodo non sia più di un giorno avanti o indietro rispetto alla data del sistema operativo sul server applicazioni.

Messaggi di credenziali non valide su Windows XP

Valido su computer con sistema operativo Windows XP.

Sintomo:

Quando vengono aggiunti nodi basati su Windows XP dalla schermata Nodo, viene visualizzato il seguente messaggio:

```
Credenziali utente non valide.
```

Soluzione:

In determinate condizioni, CA ARCserve Central Protection Manager non è in grado di aggiungere i nodi Windows XP se l'opzione Condivisione file semplice di Windows per la cartella è stata attivata. Per risolvere il problema, procedere come segue:

1. Accedere al nodo Windows XP e aprire Esplora risorse.
2. Scegliere Opzioni cartella dal menu Strumenti.

   Verrà visualizzata la finestra di dialogo Opzioni cartella.

3. Fare clic su Visualizza e selezionare Condivisione file semplice (scelta consigliata).
4. Deselezionare la casella di controllo accanto all'opzione Condivisione file semplice (scelta consigliata), quindi fare clic su OK.

   La condivisione file semplice viene disattivata.

5. Accedere al server CA ARCserve Central Protection Manager e aggiungere il nodo.

Errore di accesso negato con l'aggiunta di un nodo per IP/Nome

Valido su tutti i sistemi operativi Windows con supporto del Controllo account utente (UAC).

Nota: Windows Vista, Windows Server 2008, Windows Server 2008 R2 e Windows 7 includono il supporto UAC.

Sintomo:

In caso di aggiunta dei nodi dalla finestra di dialogo Aggiungi nodo per IP/Nome con un nuovo account utente Windows appartenente al gruppo amministratori, viene visualizzato il messaggio seguente:

```
Accesso negato. Verificare di disporre dei privilegi di amministratore e che
l'accesso al registro di sistema remoto non sia limitato dai criteri di
protezione locali del computer aggiunto.
```

Come risultato non è possibile aggiungere il nodo.

Soluzione:

Si tratta di un comportamento previsto in caso di abilitazione del Controllo account utente (UAC) su un computer con sistema operativo Windows e supporto UAC. Il Controllo dell'account utente è una funzionalità Windows che consente l'accesso remoto al computer solo agli utenti con diritti di amministratore. Per risolvere questo comportamento, procedere come segue:

Procedere come descritto di seguito:

1. Accedere al nodo utilizzando l'account amministratore.
2. Aprire il Pannello di controllo di Windows.
3. Aprire Account utente.

4. Nella schermata Modifica dell'account utente, fare clic su Modifica impostazioni di Controllo dell'account utente ed eseguire una delle operazioni seguenti:

    - **Windows Vista e Windows Server 2008:** nella schermata Modifica dell'account utente, fare clic su Attiva o disattiva Controllo account utente. Nella sezione Per aumentare la protezione del computer e renderlo più sicuro, attivare il controllo dell'account utente, deselezionare la casella di controllo accanto Per proteggere il computer, utilizzare il controllo dell'account utente e fare clic su OK.

      Riavviare il computer per applicare le modifiche apportate al Controllo dell'account utente.

    - **Windows Server 2008 r2 e Windows 7:** nella schermata Scegliere quando ricevere la notifica delle modifiche al computer, spostare l'Indicatore scorrevole da Notifica sempre a Non notificare mai. Fare clic su OK e chiudere il Pannello di controllo di Windows.

      Riavviare il computer per applicare le modifiche apportate al Controllo dell'account utente.

5. Dopo aver riavviato il computer, verificare che le configurazioni seguenti siano state applicate al nodo CA ARCserve D2D:

    - Il servizio Server di Windows è in esecuzione.
    - Il servizio Condivisione file e stampanti dispone dell'autorizzazione può comunicare mediante Windows Firewall.
    - Se il nodo non deve essere unito a un dominio, il Servizio Accesso rete può comunicare mediante Windows Firewall.
    - I valori di Criteri di protezione locali,Criteri locali, Opzioni di protezione, Accesso alla rete: modello di condivisione e protezione per gli account locali sono impostati su Classico.

6. Verificare che la configurazione seguente sia applicata sul server Protection Manager:

    - Il valore di Criteri di protezione locali,Criteri locali, Opzioni di protezione, Protezione di rete: livello di autenticazione di LAN Manager è impostato su Invia LM e NTLM. Utilizza la protezione sessione NTLMv2 se negoziata.

Viene visualizzato un errore del certificato quando si accede all'applicazione

Valido per piattaforme Windows.

Sintomo:

Quando si accede all'applicazione viene visualizzato il seguente messaggio nella finestra del browser:

- Internet Explorer

  `Si è verificato un problema con il certificato di protezione del sito Web.`

- Firefox

  `Questa connessione non è attendibile.`

- Chrome:

  `Il certificato di sicurezza di questo sito non è attendibile.`

Se si specifica un'opzione che consente di passare al sito Web, sarà possibile accedere all'applicazione. Questo comportamento, tuttavia, si verifica ogni volta che si accede all'applicazione.

Soluzione:

Questo comportamento si verifica quando si imposta l'utilizzo di HTTPS come protocollo di comunicazione. Per risolvere temporaneamente il problema, nella finestra del browser fare clic sul collegamento che consente di passare al sito Web. Al successivo accesso all'applicazione, comunque, il messaggio verrà nuovamente visualizzato.

Il protocollo di comunicazione HTTPS (sicuro) garantisce una maggiore sicurezza rispetto al protocollo di comunicazione HTTP. Se si desidera continuare a comunicare utilizzando il protocollo di comunicazione HTTPS, è possibile acquistare un certificato di sicurezza da VeriSign e quindi installare il certificato sul server applicazioni. Facoltativamente, è possibile impostare su HTTP il protocollo di comunicazione utilizzato dall'applicazione. Per impostare il protocollo di comunicazione su HTTP, procedere come segue:

1. Accedere al server in cui è installata l'applicazione.
2. Individuare la seguente directory:

   `C:\Programmi\CA\ARCserve Central Applications\BIN`

3. Eseguire il file batch seguente:

   `ChangeToHttp.bat`

4. Al termine dell'esecuzione del file batch, aprire Server Manager di Windows.

   Riavviare il seguente servizio:

   `Servizio CA ARCserve Central Applications`

Il processo di sincronizzazione di CA ARCserve Backup ha esito negativo

Valido per piattaforme Windows.

Sintomo:

Il processo di sincronizzazione di CA ARCserve Backup ha esito negativo ed è disponibile in Visualizza registro.

Soluzione:

Il processo di sincronizzazione di CA ARCserve Backup può non riuscire se lo spazio su disco non è sufficiente per l'archiviazione dei dati temporanei di sincronizzazione (file dump). Per impostazione predefinita, i file dump vengono archiviati nella directory ARCserve_Central_Applications_Home\ASBUSync.

Se lo spazio libero su disco in C:\Programmi è limitato e i file contenuti in ASBUSync occupano uno spazio superiore a quello libero disponibile su disco, non è possibile recuperare i dati dump del database CA ARCserve Backup necessari per completare il processo di sincronizzazione. Di conseguenza, il processo di sincronizzazione di CA ARCserve Backup ha esito negativo.

Facoltativamente, l'applicazione consente di specificare un percorso alternativo per archiviare i dati di sincronizzazione di CA ARCserve Backup. Per correggere il problema o evitare che si verifichi, procedere come segue:

1. Accedere al server di CA ARCserve Central Protection Manager.
2. Aprire l'editor del Registro di sistema di Windows e individuare la seguente chiave:

   `HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve Central Application\CM`

3. Fare clic con il pulsante destro del mouse su CM, scegliere Nuovo e quindi Valore stringa dal menu di scelta rapida.

   Assegnare alla chiave il nome seguente:

   `ARCserveSyncPath`

4. Fare clic su ARCserveSyncPath, quindi su Modifica nel menu a comparsa.

   Viene visualizzata la finestra di dialogo di modifica della stringa.

5. Nel campo Dati valore specificare la posizione in cui si desidera archiviare i dati di sincronizzazione di CA ARCserve Backup.

   Fare clic su OK.

Viene specificato il percorso alternativo.

Errore delle operazioni di ridistribuzione di CA ARCserve D2D

Valido per piattaforme Windows.

Sintomo:

Durante le operazioni di ridistribuzione dei nodi CA ARCserve D2D, il processo di distribuzione viene completato correttamente. Questo comportamento si verifica se si produce uno degli eventi seguenti:

- Uno dei messaggi seguenti viene visualizzato in Stato della distribuzione della finestra di dialogo Distribuzione D2D:

  `Accesso non riuscito.`

  `Sul computer di destinazione potrebbe essere presente la stessa versione, una versione più recente o una versione non supportata del prodotto. Prima di installare la versione corrente del prodotto, disinstallare la versione precedente dal computer di destinazione.`

  `Impossibile copiare i file sul computer remoto.`

- Il nodo, pertanto, non viene visualizzato nella schermata Nodo.
- Nella schermata Nodo, lo stato del nodo visualizzato non è corretto. Ad esempio, nella schermata Nodo viene visualizzata l'icona , oppure l'icona non viene visualizzata nella schermata.

Soluzione:

Questi evento si verifica nei seguenti casi:

- Riavvio o interruzione del servizio Web di CA ARCserve Central Applications durante il processo di distribuzione e mancato riavvio del server di destinazione in seguito all'installazione di CA ARCserve D2D.
- Riavvio del servizio Web di CA ARCserve Central Applications durante il processo di distribuzione e mancato riavvio del server di destinazione in seguito all'installazione di CA ARCserve D2D.

Per risolvere questo problema, eseguire le operazioni seguenti:

1. Accedere al server D2D e riavviare il server.
2. Accedere a Central Protection Manager ed effettuare una delle attività seguenti:
   - Aggiornare il nodo, nel caso in cui il nodo venga visualizzato nell'elenco dei nodi della schermata Nodo con uno stato non corretto.

     Per aggiornare il nodo, selezionare il nodo e fare clic su Aggiorna dal menu di popup.
   - Se il nodo non viene visualizzato nell'elenco dei nodi della schermata Nodo, aggiungere il nodo manualmente.

     Per aggiungere il nodo manualmente, selezionare Aggiungi dalla barra degli strumenti e fare clic su Aggiungi nodo per IP/Nome dal menu di popup.

Risoluzione dei problemi relativi al caricamento delle pagine

Valido per piattaforme Windows.

Sintomo:

La finestra del browser visualizza i messaggi di errore riportati di seguito quando viene eseguito l'accesso ai nodi CA ARCserve Central Applications e CA ARCserve D2D e ai server di monitoraggio.

Messaggio 1:

```
Gli errori presenti nella pagina Web potrebbero impedirne il corretto
funzionamento.
```

Messaggio 2:

```
!
```

Soluzione:

Il caricamento delle pagine Web non viene eseguito correttamente per diverse ragioni. Nella tabella seguente sono descritte le cause più comuni e le corrispondenti misure correttive:

Motivo	Misura correttiva
Si sono verificati problemi relativi al codice sorgente HTML sottostante.	Aggiornare la pagina Web e riprovare.
La rete blocca l'esecuzione degli script attivi, i controlli ActiveX o i programmi Java.	Consentire al browser di utilizzare gli script attivi, i controlli ActiveX o i programmi Java.

Motivo	Misura correttiva
L'applicazione antivirus è configurata per la scansione dei file temporanei Internet e dei programmi scaricati.	Applicare un filtro nell'applicazione antivirus in modo da consentire i file Internet associati alle pagine Web di CA ARCserve Central Applications.
Il motore di script installato nel computer è danneggiato o non è aggiornato.	Aggiornare il motore di script.
I driver della scheda video installati nel computer sono danneggiati o non sono aggiornati.	Aggiornare i driver della scheda video.
Il componente DirectX installato nel computer è danneggiato o non è aggiornato.	Aggiornare il componente DirectX.

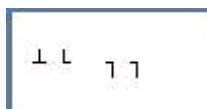
Visualizzazione di caratteri corrotti nella finestra del browser durante l'accesso a CA ARCserve Central Applications

Valido per tutti i sistemi operativi Windows e per tutti i browser.

Sintomo:

Quando viene eseguito l'accesso a CA ARCserve Central Applications, vengono visualizzati caratteri corrotti nell'area di contenuto della finestra del browser.

Soluzione:

Questo problema si verifica nel caso in cui l'installazione di CA ARCserve Central Applications sia stata eseguita mediante comunicazione HTTPS e l'accesso a CA ARCserve Central Applications mediante comunicazione HTTP. Il componente dei servizi Web sottostanti di CA ARCserve Central Applications non supporta la funzionalità di conversione degli URL HTTP in HTTPS. Di conseguenza, i caratteri corrotti vengono visualizzati nella finestra del browser. Ad esempio:

Per correggere il problema, accedere a CA ARCserve Central Applications utilizzando il protocollo HTTPS per l'installazione o la configurazione delle applicazioni di comunicazione che utilizzano tale protocollo.

I nodi non compaiono nella schermata Nodi dopo la modifica del nome del nodo

Valido per piattaforme Windows.

Sintomo:

Il nome host del nodo è stato modificato dopo l'aggiunta alla schermata Nodo. Il nodo non viene più visualizzato nella schermata Nodo.

Soluzione:

Si tratta di un comportamento normale. CA ARCserve Central Protection Manager conserva il nome del nodo aggiunto dalla schermata Nodo. Quando si rinomina il nodo, l'applicazione non è in grado di rilevare il nodo. Il nodo, pertanto, non viene visualizzato nella schermata Nodo.

Per visualizzare i nodi rinominati nella schermata Nodo, procedere come segue:

1. Rinominare il nodo.
2. Aprire la schermata Nodo ed eliminare il nodo (a pagina 70) rinominato.
3. Aggiungere il nodo (a pagina 64) utilizzando il nuovo nome.

Problemi di comunicazione di CA ARCserve Central Protection Manager con il servizio Web CA ARCserve D2D su nodi remoti

Applicabile ai sistemi operativi Windows.

Sintomo:

CA ARCserve Central Protection Manager non è in grado di stabilire la comunicazione con il servizio Web CA ARCserve D2D su nodi remoti.

Soluzione:

La seguente tabella descrive i motivi per cui CA ARCserve Central Protection Manager non è in grado di stabilire la connessione con il servizio Web CA ARCserve D2D sui nodi remoti e indica le azioni correttive corrispondenti:

Causa	Misura correttiva
La rete non è disponibile o non è stabile durante l'applicazione dei criteri.	Verificare che la rete sia disponibile e stabile e riprovare.

Causa	Misura correttiva
Il computer di CA ARCserve D2D non è in grado di gestire il carico quando l'applicazione tenta di stabilire la comunicazione con il nodo.	Verificare che lo stato della CPU sul nodo di CA ARCserve D2D si normalizzi e riprovare.
Durante la distribuzione dei criteri, il servizio CA ARCserve D2D non è in esecuzione sul nodo remoto.	Verificare che CA ARCserve D2D sia in esecuzione sul nodo remoto e riprovare.
Si verificano problemi di comunicazione del servizio CA ARCserve D2D.	Riavviare il servizio CA ARCserve D2D sul nodo remoto e riprovare.

I nodi non sono gestiti dopo la distribuzione D2D

Valido per piattaforme Windows.

Sintomo:

Quando si distribuisce CA ARCserve D2D su un nodo di un server remoto o locale, il nodo viene aggiunto al gruppo di nodi ma lo stato corrisponde a Non gestito.

Il problema si verifica con una delle seguenti condizioni:

- CA ARCserve D2D è stato distribuito su un nodo remoto senza aver eseguito il riavvio.
- CA ARCserve D2D è stato distribuito sul server CA ARCserve Central Applications con o senza l'esecuzione del riavvio.

Soluzione:

Per risolvere il problema, riavviare il server CA ARCserve D2D e aggiornare le informazioni relative al nodo CA ARCserve D2D in CA ARCserve Central Protection Manager. Lo stato diventa gestito.

Impostazione delle pianificazioni per l'eliminazione dei dati del nodo.

Valido per piattaforme Windows.

Sintomo:

Per impostazione predefinita, la pianificazione dell'eliminazione dei dati del nodo è impostata su ogni giorno alle 2.00. L'utente desidera personalizzare la pianificazione per l'eliminazione di più dati.

Soluzione:

Per creare una pianificazione personalizzata per l'eliminazione dei dati del nodo, impostare il valore della chiave di registro CA ARCserve Central Applications\CM\ShowDeleteNodeConfigurationUI su 1. L'impostazione della chiave di registro su 1 consente di aggiungere la scheda Configurazione eliminazione dei dati del nodo al riquadro Configurazione dell'applicazione CA ARCserve Central Protection Manager. In tal modo è possibile modificare la pianificazione.

Nota: per accedere al registro, eseguire l'accesso direttamente al server CA ARCserve Central Protection Manager, quindi selezionare Start > Esegui > Regedit.

Errore di avvio dei servici del database CA ARCserve Central Applications

Valido per piattaforme Windows e Microsoft SQL Server e per database Microsoft SQL Server Express Edition.

Sintomo:

Quando si procede all'avvio o al riavvio del server CA ARCserve Central Protection Manager o del server su cui è installato il database CA ARCserve Central Applications, si verifica un errore di avvio dei servizi del database CA ARCserve Central Applications.

Soluzione:

Quando si procede all'avvio di un computer, i servizi segnalano il proprio stato di avvio al sistema operativo. Se il sistema operativo non riceve alcun segnale entro un determinato intervallo di tempo (periodo di timeout), i servizi vengono interrotti da Windows. Per impostazione predefinita, quando i servizi CA ARCserve Central Applications non segnalano il proprio stato entro 30 secondi dall'ora di inizio, Windows interrompe i servizi del database. È molto probabile che problemi di questo tipo si verifichino quando il database è installato su un server con risorse insufficienti. Ad ogni modo, è possibile prevenire il problema aumentando il periodo di timeout dell'avvio. Per aumentare l'intervallo di timeout, procedere come segue:

1. Aprire l'editor del Registro di sistema di Windows e cercare la seguente chiave:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`
2. Fare clic con il tasto destro del mouse su Controllo, Nuovo, quindi su Chiave dal menu di scelta rapida.

   Viene creata una chiave New Key #1.
3. Rinominare New #1 come segue: ServicesPipeTimeout.
4. Fare clic su ServicesPipeTimeout, quindi su Modifica nel menu a comparsa.

   Viene visualizzata la finestra di dialogo Modifica valore DWORD.
5. Nel campo di dati Valore, specificare il valore che si desidera impostare per il periodo di timeout. Indicare il valore in millisecondi. Ad esempio, per impostare il periodo di timeout su 60 secondi, specificare 60000 nel campo di dati Valore.

   Nota: Un secondo equivale a 1000 millisecondi.

   Fare clic su OK.

   Il periodo di timeout viene applicato.
6. Per rendere effettive le modifiche su Windows, riavviare il computer.

Errore di connessione multipla durante il salvataggio o l'assegnazione di un criterio a un server CA ARCserve D2D.

Applicabile a tutte le piattaforme Windows.

Sintomo:

Durante il tentativo di salvataggio o a assegnazione di un criterio a un server CA ARCserve D2D, viene visualizzato il messaggio di errore seguente:

```
Convalida della destinazione di backup non riuscita. Le connessioni multiple a un
server o ad una risorsa condivisa da parte di uno stesso utente con vari nomi
utente non sono consentite. Disconnettere tutte le connessioni precedenti al
server o alla risorsa condivisa e riprovare.
```

Soluzione:

Se il messaggio precedente viene visualizzato quando si tenta di eseguire il salvataggio o a l'assegnazione di un criterio a un server CA ARCserve D2D, è possibile procedere come segue per risolvere il problema:

- Specificare il campo Nome utente in formato "nome computer (o dominio)\nomeutente".
- Individuare il server remoto della cartella condivisa ed eliminare tutte le sessioni dal server CA ARCserve Central Applications o dal server CA ARCserve D2D. Per eliminare le sessioni, procedere come segue:
  - Eseguire il comando:

    ```
    net session \\machinename /delete
    ```

  - Disconnettere la sessione nella directory seguente:

    ```
    Compmgmt.msc > Utilità di sistema > Cartelle condivise > Sessioni >
    Disconnetti sessione
    ```

- Assicurarsi di utilizzare lo stesso nome utente per accedere alla cartella condivisa remota.
- Salvare, quindi effettuare nuovamente la distribuzione del criterio.

Errore delle operazioni di distribuzione dei criteri e sincronizzazione dei dati.

Valido per piattaforme Windows.

Sintomo:

Dopo aver avviato le operazioni di sincronizzazione dei dati CA ARCserve D2D, viene visualizzato il seguente messaggio nel registro attività:

```
Impossibile accedere al servizio CA ARCserve D2D.
```

Durante la distribuzione di un criterio sul nodo, viene visualizzata la seguente finestra di messaggio:

```
Deploy policy failed (failed to connect to the node) (Distribuzione del criterio
non riuscita. Impossibile stabilire la connessione al nodo).
```

Soluzione:

Questo comportamento si verifica in caso di disinstallazione di CA ARCserve D2D dal nodo dopo aver eseguito la sua registrazione sul server CA ARCserve Central Protection Manager e aver reinstallato manualmente CA ARCserve D2D sul nodo. Questo comportamento non si verifica se la reinstallazione di CA ARCserve D2D sul nodo viene eseguita mediante l'utilità di distribuzione di CA ARCserve Central Protection Manager.

Per risolvere questo comportamento, aggiornare il nodo dalla schermata Nodo. Per aggiornare il nodo, selezionare il nodo e fare clic su Aggiorna dal menu di popup. Completare i campi obbligatori della finestra di dialogo Aggiorna nodo.

Risoluzione problemi per numero di errore

La tabella seguente descrive i numeri di errore visualizzati come messaggi popup quando si procede all'aggiunta o all'aggiornamento di nodi mediante CA ARCserve Central Protection Manager.

Numero errore	Descrizione	Soluzione possibile
12884901933	Impossibile stabilire una connessione con il servizio di CA ARCserve D2D su *** con numero di errore 12884901933. Verificare che tutte le voci del nodo siano corrette e che il servizio di CA ARCserve D2D sia in esecuzione.	Verificare che: ■ Il servizio di CA ARCserve D2D sia in esecuzione sul nodo. ■ Il nome host, l'indirizzo IP e il protocollo di comunicazione specificati per il nodo siano corretti. ■ Il servizio Web di CA ARCserve D2D sul nodo sia in esecuzione e non bloccato a causa si un errore di risoluzione dell'indirizzo IP del nodo da parte del DNS. ■ Il servizio Web di CA ARCserve D2D sul nodo sia in esecuzione e il firewall di Windows, o qualsiasi altro firewall, non stiano bloccando la comunicazione. ■ Il cavo di rete connesso al nodo stia funzionando correttamente. ■ L'utente che accede al nodo disponga delle autorizzazioni richieste per la comunicazione mediante una rete senza fili.
12884901935	Impossibile stabilire una connessione con il servizio di CA ARCserve Backup su *** con numero di errore 12884901935. Verificare che tutte le voci del nodo siano corrette e che il servizio di CA ARCserve Backup sia in esecuzione.	Verificare che il servizio CA ARCserve Communication Foundation sia in esecuzione sul nodo.
12884901936	Impossibile stabilire una connessione con il servizio di CA ARCserve Backup su *** con numero di errore 12884901936. Verificare che CA ARCserve Central Applications supporti la versione del servizio di CA ARCserve Backup installata sul nodo.	Verificare che: ■ CA ARCserve Central Applications supporti la versione del servizio di CA ARCserve Backup installata sul nodo. ■ Il servizio CA ARCserve Communication Foundation sia in esecuzione sul nodo.

Collegamento Aggiungi nuova scheda non funzionante per Internet Explorer 8, 9 e Chrome.

Valido per Windows

Sintomo:

Quando viene aggiunto un nuovo collegamento alla scheda della barra di navigazione specificando un URL HTTPS, facendo clic sulla nuova scheda verranno visualizzati i seguenti messaggi di errore:

- Internet Explorer 8 e 9:

  `Il contenuto è stato bloccato poiché non è stato firmato da un certificato di protezione valido.`

- Chrome:

  `La pagina Web non è disponibile.`

Soluzione:

Per correggere il problema relativo a Internet Explorer, eseguire le seguenti operazioni:

- Internet Explorer 8:

  Fare clic sulla barra del messaggio e selezionare Visualizza contenuto bloccato.

- Internet Explorer 9:

  Fare clic sul pulsante Mostra il contenuto della Barra messaggi nella parte inferiore della pagina. La pagina viene aggiornata e il collegamento alla scheda aggiunta viene aperto correttamente.

Per risolvere il problema relativo a Chrome, eseguire le seguenti operazioni:

Fase 1 - Esportazione del certificato:

1. Aprire una nuova scheda in Chrome ed immettere l'URL HTTPS.

   Verrà visualizzato il messaggio di avviso "Il certificato di sicurezza del sito non è affidabile!"

2. Dalla barra degli indirizzi, fare clic sul lucchetto contrassegnato con una X.

   Verrà visualizzata una finestra popup contenente il collegamento a Informazioni sul certificato.

3. Fare clic sul collegamento Informazioni sul certificato.

   Verrà visualizzata la finestra di dialogo Certificato.

4. Fare clic sulla scheda Dettagli, quindi selezionare Copia su file per salvare il certificato sul computer locale.

   Viene visualizzata la procedura guidata di esportazione del certificato.

5. Fare clic su Avanti per selezionare il formato desiderato per l'esportazione del file.

   Nota: X.509 binario codificato DER (.CER) è selezionato per impostazione predefinita.

6. Fare clic su Avanti per selezionare un percorso in cui salvare il certificato.
7. Fare clic su Avanti per completare la procedura guidata di esportazione del certificato, quindi fare clic su Fine.

Il certificato viene esportato correttamente.

Fase 2 - Importazione del certificato:

1. Selezionare Opzioni da Personalizza e controlla Google Chrome.

   Verrà visualizzata la finestra di dialogo Opzioni.

2. Selezionare l'opzione Roba da smanettoni, quindi selezionare Gestisci certificati della sezione HTTPS/SSL.

   Viene visualizzata la finestra di dialogo Certificati.

3. Fare clic su Importa.

   Viene visualizzata la procedura guidata di importazione del certificato.

4. Fare clic su Avanti per ricercare il certificato salvato sul computer locale.
5. Fare clic su Avanti per aprire l'Archivio certificati.

   Verrà visualizzata la finestra di dialogo Archivio certificati.

6. Fare clic su Sfoglia per aprire la finestra di dialogo Selezione archivio certificati.

   Viene visualizzata la finestra di dialogo Selezione archivio certificati.

7. Selezionare Autorità di certificazione fonti attendibili dall'elenco di file, quindi fare clic su OK.

   Viene visualizzata la finestra di dialogo Archivio certificati.

8. Fare clic su Avanti per completare la procedura guidata di importazione del certificato, quindi fare clic su Fine.

   Verrà visualizzata una finestra di dialogo di avviso che comunica all'utente che si sta per installare un certificato.

   Fare clic su Sì per accettare i termini.

Il certificato viene importato correttamente.

Collegamento Aggiungi nuova scheda, Feed RSS e commenti relativi al social network non avviati correttamente in Internet Explorer 8 e 9

Valido per Windows

Sintomo:

Per un URL CA ARCserve Central Applications HTTPS:

Quando viene aggiunto un nuovo collegamento alla scheda della barra di navigazione specificando un URL HTTP, facendo clic sulla nuova scheda e sul collegamento Commenti e suggerimenti verranno visualizzati i seguenti messaggi di errore:

```
La navigazione alla pagina Web è stata annullata.
```

Inoltre, i feed RSS non vengono visualizzati.

Nota: il collegamento Commenti e suggerimenti visualizza un messaggio di errore anche se non viene aggiunto il collegamento alla nuova scheda.

Soluzione:

Per risolvere il problema, procedere come segue:

- Internet Explorer 8:

  Dopo aver eseguito l'accesso, viene visualizzato il messaggio di avviso Visualizzare solo le informazioni della pagina Web fornite in modo protetto? Selezionare No per visualizzare il contenuto non protetto della pagina Web.

- Internet Explorer 9:

  Fare clic sul pulsante Mostra tutto il contenuto della barra dei messaggi nella parte inferiore della pagina. La pagina viene aggiornata e il collegamento alla scheda aggiunta viene aperto correttamente.

Visualizzazione incorretta dei caratteri provenienti da server localizzati nella console di allarme di Nimsoft UMP

Valido per Windows

Sintomo:

I caratteri dei messaggi di avviso ricevuti dai server localizzati vengono visualizzati come testo confuso nella console di allarme di Nimsoft Unified Monitoring Portal (UMP).

Soluzione:

Questo comportamento si verifica quando il set di caratteri utilizzati sul server di invio degli avvisi è diverso dal set di caratteri utilizzato sul server Nimsoft. Per risolvere il problema, configurare il server Nimsoft per l'utilizzo della codifica UTF-8. Per configurare il server Nimsoft per l'utilizzo della codifica UTF-8, procedere come segue:

1. Verificare che il modulo di dashboard sia configurato per l'utilizzo di –Dfile.encoding=utf-8 come parametro di avvio
2. Verificare che l'opzione di argomento del computer virtuale Java aggiuntivo WASP sia definita come -Dfile.encoding=utf-8.

Nota: per ulteriori informazioni, consultare la documentazione di Nimsoft.

Indice

A

B

C

D

O

P

R

S

U

V